SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1986-87

© Minister of Supply and Services Canada 1987

Cat. No. JS71-1/1987

ISBN 0-662-55252-0

Security Intelligence Review Committee
14th Floor
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

(613) 990-8441: Collect calls are accepted, and the switchboard is open from 7:30 a.m. to 6 p.m., Ottawa time.

The quotation from *The RCMP and the Management of National Security* appears with the permission of the Institute for Research on Public Policy.

June 22, 1987

The Honourable James F. Kelleher, P.C., M.P., Q.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Kelleher:

Pursuant to section 53 of the *Canadian Security Intelligence Service Act*, we hereby transmit to you the annual report of the Security Intelligence Review Committee for the fiscal year 1986-87, for submission to Parliament.

Yours sincerely,

Ronald G. Atkey, P.C., Q.C.
Chairman

Jean Jacques Blais, P.C., Q.C.

Frank McGee, P.C.

Saul M. Cherniack, P.C., Q.C.

Paule Gauthier, P.C.

Quis custodiet ipsos custodes?

(Who is to guard the guards themselves?)

Juvenal

Contents

1. **Introduction** 1

Mandate 1
Relations with CSIS 2
How We Operate 2
On the Record 3
Balance 3

2. **Oversight** 5

Formal Controls 5
Ministerial Instructions 6
CSIS Annual Report and Certificate of the Inspector General 6
The Oversight Process 7

3. **How CSIS Knows** 9

Behind Federal Court Warrants 9
Counting Them Up 10
Other People's Mail 11
Emergency Warrants 12
Open Sources 12
Canadian Police Information Centre 14
Academe and Officialdom 15
Inter-Organizational Arrangements in Canada 16
Foreign Arrangements 17
Unlawful Acts 18

4. **What CSIS Knows** 21

Legal Limits 21
Inherited Information 21
Retirement of Old Files 22
Foreign Intelligence 23
Incidental Information 24

5. **What CSIS Does** 25

Spin-Off Information 25
CSIS in Court 25
Assistance to Police 26
Relations with the RCMP 27
Airport Security Alert 28
Foreign Liaison Officers 29
Persona Non Grata 29
The Public Interest 30
Front Organizations 30

6. Counter-Subversion Operations 33

Principles and Law 33
How We Proceeded 34
Transition 34
Resources 35
Human Sources 35
Targeting 35
Files on Individuals 38
Dissemination of Information 39
Five Organizations 39
Two Paths 40

7. CSIS Itself 41

Resources and Administration 41
Civilianization 42
Who Is Recruited 43
Time Out at the Academy 44
Bilingualism and Equitable Participation 44
The First Class 45
Building Morale 46
Polygraph Examinations 46

8. Closing the Gaps 49

Official Languages 49
Staff Relations 52

9. Complaints 55

Kudos for Defence 55
Security Clearances 55
Complaints against CSIS 56
Immigration and Citizenship 57
Quality of Investigations 57
Immigration Act Study 59
The New Security Policy 59

10. Tidying Up 63

Answering to Parliament 63
Outreach 63
Meetings and Conferences 63
Personnel 64
Financial Report 64

11. Looking Ahead 67

Five-Year Review 67
The Extent of Oversight 67
A Last Word 69

Appendices

A: Ministerial Directives and Directions, 1986-87 71
B: Case Histories 73
C: SIRC Personnel 77

1. Introduction

Independent, external review of security intelligence is a recent development in all the democracies. Here in Canada, it goes back only three years, to 1984, when Parliament adopted the *Canadian Security Intelligence Service Act (CSIS Act)*.

Under this *Act*, the responsibilities of the RCMP Security Service were transferred to a new Canadian Security Intelligence Service (CSIS). Our Committee, the Security Intelligence Review Committee (SIRC), was appointed to provide external oversight. An Inspector General was appointed to provide internal oversight and to report to the Solicitor General.

As pioneers entering a new area of public administration, we first faced the challenge of finding our bearings. This was very much reflected in our first two annual reports.

However, we are now beginning to zero in as we pass the mid-point of our five-year mandate. We are now equipped to analyse statistics on CSIS operations, to detect trends. We have also carried out major studies—on counter-subversion, for example—in addition to pursuing dozens of issues through written inquiries and interviews with CSIS officials.

On Course. We hope that readers of this annual report will share the sense that external review is now firmly on course. We touch on more topics and do so in greater depth than in our two previous reports.

Some themes will be familiar from our past reports. Our firm belief that CSIS is not making enough use of open sources as an alternative to covert investigations is just one example. We have also continued to report the total number of new warrants and renewals granted to CSIS by the Federal Court of Canada.

Among the subjects we have examined in greater depth are the counter-subversion program, particularly the way targets are chosen, relations between CSIS and the RCMP in counter-terrorism operations, and civilianization.

We feel mounting concern that civilianization is proceeding too slowly because of heavy recruitment of ex-police-officers. This can only perpetuate the law-enforcement approach that Parliament intended to change when it adopted the *CSIS Act*.

Mandate

In general terms, our mandate is to see that the Service carries out its work effectively but without unreasonable or unnecessary intrusions on individual rights. Specific tasks spelled out for us in the *CSIS Act* fall into two broad areas—oversight and complaints.

Oversight. Paragraph 38(*a*) of the *CSIS Act* directs us "to review generally the performance by the Service of its duties and functions" while paragraph 38(*b*) and section 40 permit us "to arrange for reviews to be conducted, or to conduct reviews" with a view to "ensuring that the activities of the Service are carried out in accordance with this *Act*, the regulations and directions issued by the Minister ... and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers".

Chapters 2-8 of this report describe what we did last year to fulfil our oversight mandate.

Oversight does not mean that we are a kind of board of directors for CSIS. We do not hesitate to give advice, privately when circumstances dictate and publicly, when we can, through our annual reports and in testimony before Parliamentary committees.

But we do not set policy or issue orders. Nor would we want to, for that would make us active players in security intelligence and remove the freedom to criticize that is our *raison d'être*.

Complaints. Paragraph 38(*c*) directs us to investigate complaints that anyone makes about the activities of the Service, complaints about the denial of security clearances in Public Service employment, in the supply of goods and services to the federal government and in immigration and citizenship matters, as well as to investigate the security aspects of certain complaints lodged with the Canadian Human Rights Commission.

Chapter 9 of this report covers our work in this area, and summary case histories are set out in Appendix B.

Relations with CSIS

The price of our independence is an arm's-length relationship with CSIS and other participants in the Canadian security intelligence establishment.

Independent, external oversight is the price that CSIS pays for its wide powers.

The Service provides us with the information we ask for, but it remains distant and wary. This is not necessarily a bad thing; too close a relationship could make it difficult for us to maintain our independence.

How We Operate

The *CSIS Act* provides that members of our Committee shall be appointed by the Governor in Council following consultations by the Prime Minister with the Leader of the Opposition and the leader of each party with 12 or more members in the House of Commons.

In making the initial appointments, the Prime Minister gave these consultations a very wide scope and invited the Leader of the Opposition and the Leader of the New Democratic Party to nominate one member each while he himself nominated three members. The approval of all three leaders was sought for the complete slate. As a result, our Committee is clearly tri-partisan.

Once the appointment process was completed, however, we found it desirable to leave partisan considerations at the door. For the most part, we operate collegially, by consensus, in our oversight role. Also, the fact that we are part-timers, active in our communities and in private life, outside of government circles in Ottawa, makes it easier to focus on our task in a non-partisan way when we meet.

Complaints are usually heard by a single Committee member. While we all see the final reports, we provide legal and editorial comments only. We do not seek to discuss or amend the rationale or conclusions, following the rule that only the person who has heard the evidence at first hand can give each element in the case its proper weight. Under our conflict of interest rules, no Committee member participates at all in a case in which he or she has any advance knowledge of or association with the individual concerned.

On the Record

We have made Juvenal's much-quoted line "Who is to guard the guards themselves" the epigraph of this report. We were thinking of our relationship with CSIS. But it could be applied to us too. Parliament and Canadians must rely in large part on our Committee and the Inspector General to ensure that individual rights and freedoms are protected in the security intelligence field.

That is why, in preparing our annual report, we try to put as much as possible on the public record. The more we tell, the better Parliament and Canadians will be able to judge for themselves.

We are, of course, constrained by the statutory requirement to avoid revealing anything that would compromise national security. Under the *Act*, CSIS reviews the draft report and advises us about any information that it believes might do so. Some detailed supporting information is left out of the published report as a result of this process, but we do not feel that anything of great significance has been lost.

Balance

Annual reports by oversight or auditing bodies usually provide a litany of criticisms rather than a balanced picture. This is to be expected.

In addition, our annual report is constrained by our inability to comment on CSIS's successes, for national security reasons. There have been a number of successes, particularly in the fields of counter-espionage and counter-terrorism.

This report is not, therefore, a complete picture; it is a view through slightly parted curtains. If we were able to pull the drapes wide open, we would include much more information on the important and effective work accomplished day in, day out by the Service. It is an important national institution worthy of continued public support.

The dedication and professionalism of CSIS employees is impressed upon us anew at every contact we have with them from one end of the country to the other.

2. Oversight

Does CSIS protect the national interest as effectively as possible? Is it efficient—in terms of both management goals like financial integrity and policy goals like "civilianization" and official bilingualism? Does it give enough weight to individual rights and freedoms?

In its simplest terms, our oversight mandate is to keep a running score on these questions on behalf of Parliament and the Canadian people. Our particular role is to watch over the delicate balance between national security and individual freedoms.

Oversight is the topic of this chapter and the six that follow. We begin with formal controls on CSIS. We then deal with various issues loosely grouped under three headings: gathering information, managing information and putting information to use. An in-depth study that we made of CSIS's counter-subversion program overlaps all these themes, so it has a chapter of its own. We conclude with a review of some internal management issues and a chapter on a major study that we undertook, at the request of the Solicitor General, on official languages and staff relations issues in CSIS.

Formal Controls

Because of its wide powers of investigation and the secrecy that unavoidably surrounds much of its work, CSIS comes under a variety of controls, both judicial and administrative.

Before using its most intrusive powers, it must convince a judge of the Federal Court of Canada to issue a warrant (Part II of the *CSIS Act*). Indeed, it must first convince the Solicitor General, whose personal approval is required for each warrant application.

There are a number of other circumstances when CSIS requires the personal consent of the Solicitor General to do something—before it enters into an agreement with a province, for example (section 17 of the *Act*).

In addition, the Solicitor General issues instructions to CSIS on the conduct of particular cases or of entire classes of cases (subsection 6(2) of the *Act*).

The Solicitor General has his own watchdog on CSIS, the Inspector General (sections 30-33 of the *Act*). The Inspector General issues an annual certificate setting out whether he is satisfied with the secret annual report that the Director of CSIS makes to the Solicitor General, whether the Service has remained within the *Act* and the Solicitor General's instructions in its operational activities and whether it has made unreasonable or unnecessary use of its powers.

Our oversight mandate takes in all these controls (section 38 of the *CSIS Act*). We examine the Solicitor General's instructions, the annual report of the Director and the certificate of the Inspector General, and we keep an eye on warrants.

Warrants are dealt with in the next chapter. In this chapter we briefly report our observations on the other formal controls.

Ministerial Instructions

Two kinds of instructions are issued by the Solicitor General—ministerial directives and ministerial direction. Directives are policy statements, laying down how operations of a given class are to be handled. They usually require that certain matters be referred to the Solicitor General for decision on a case-by-case basis.

Direction, on the other hand, typically takes the shape of correspondence on specific cases, in which the Solicitor General may incidentally provide policy guidance or establish precedents that can be applied to other cases.

In last year's annual report, we indicated that we had a number of outstanding questions after reviewing the Compendium of Ministerial Direction containing all known directives and direction to the former RCMP Security Service and to CSIS. We are satisfied with the answers that CSIS and the Ministry of the Solicitor General have given us since then.

We also indicated last year that CSIS was reviewing the Compendium, looking for things that might have to be amended to conform with the *CSIS Act*. We understand that the task is now nearly complete, and we look forward to receiving the results.

New Business. We received copies of nine new directives and directions in 1986-87. A list can be found in Appendix A to this report. Two arrived late in March, and we were unable to examine them before the end of the fiscal year under review. We are satisfied that those we had a chance to study do not involve any unreasonable or unnecessary use of the Service's powers, nor do they impinge unduly on individual rights or privacy.

The Solicitor General also advised us in 1986-87 that seven directives and directions had been withdrawn. One, dealing with security assessments, has been replaced with new instructions. The others had also been overtaken by events.

As part of our review of statistics on operational activities, we now monitor the number of operations approved by ministerial directives. This will bring to light any significant changes that we need to look into more deeply.

From our experience, we are able to say that operations so sensitive that they require explicit ministerial authority are not numerous.

However, we discovered during 1986-87 that we had not been receiving copies of all documents that we consider ministerial directives or ministerial directions. The difficulty lay in a narrow interpetation that was being given to the legal description of these instructions.

At our request, CSIS is now reviewing all correspondence with the Solicitor General so gaps in our files can be filled in and we do not face the same problem again.

CSIS Annual Report and Certificate of the Inspector General

We have examined both the annual report of the Director to the Solicitor General and the certificate of the Inspector General for the calendar year 1986, and we are satisfied that they provide a realistic overview of the Service's work.

Because of their classification—Secret in the case of the annual report, Top Secret in the case of the certificate—we cannot disclose their contents.

However, what we learned from them has provided additional depth to the observations we make on our own authority in this report and will help to guide our continuing oversight activities.

We take this occasion to express our appreciation for the energy, industry and thoroughness shown by the Inspector General.

The Oversight Process

We conclude this chapter with a few facts about our oversight operations generally.

Computer Age. We entered the computer age in 1986-87, getting the data-processing capacity we need to carry out our mandate "to compile and analyse statistics on the operational activities of the Service" (subparagraph 38(*a*)(vii) of the *CSIS Act*).

Security considerations put a strict limit on how much we can say about what we learn through statistical analysis.

However, we have continued our practice of reporting warrant statistics (page 10 of this report). And statistical analysis also lies behind much of what we say about the extent to which CSIS has used various investigative tools, the CSIS budget and spending, the effects of the *CSIS Act* on operations, and progress towards civilianization.

The value of statistical analysis is that it gives us a basis for putting pertinent questions to CSIS without requiring us to undertake the impossible task of examining every operation.

Statistics have been secured from CSIS on resource allocation, warrants, the use of sources, campus operations, personnel, the targeting of groups and individuals for investigation, illegal acts and other matters. Most data is provided on a quarterly basis.

In most fields, we had data for only one quarter in 1986-87, so our analytical work was necessarily limited. It was, of course, impossible in these cases to plot trends. As we accumulate more information, we expect statistical analysis to be an important tool in oversight.

None of the data we have seen suggested an unreasonable or unnecessary use by the Service of its powers.

Formal Inquiries. We make formal, written inquiries to CSIS—145 of them in 1986-87. At year-end, only 18 were awaiting answers.

We derive our questions from many sources. Some are suggested by our own research, of course, and some emerge from our investigation of complaints.

Others are prompted by news reports—for example, in 1986-87, stories about alleged fund-raising for Contra rebels in Nicaragua, recruiting by the white-supremacist Aryan Nation, alleged surveillance of a peace activist who met with a suspected Soviet agent, immigration applications from people alleged to have been involved in torture and murder in Chile, and many more.

We kept a watching brief on investigation of the Air India disaster of June 23, 1985. There is, unfortunately, nothing we can say publicly, beyond giving an assurance that we will continue to follow developments.

We also pursue with CSIS questions put to the Director by members of Parliamentary committees, which he cannot answer in such public forums. Some of those that came up when the Standing Committee of the House of Commons on Justice and Solicitor General questioned the Director on December 11, 1986, have been answered to our satisfaction; we are waiting for responses to the rest.

Briefings. We met as a Committee with the Solicitor General, and the Chairman met frequently with the Solicitor General, the Deputy Solicitor General, the Director of CSIS and the Inspector General.

We make a point of holding our regular meetings in various cities across Canada, and we take advantage of these occasions to visit local CSIS offices, where we meet management and staff and are briefed on operations. In 1986-87, we visited the Ottawa Region, the Prairie Region in Edmonton, the Atlantic Region in Halifax, the Quebec Region in Montreal and the Toronto Region.

Our visit to Montreal came in November, in the last stages of our special study on official languages and staff relations in CSIS (reviewed in Chapter 8). Discussions with both managers and staff there helped give us a feel for the situation when we sat down to write our report on this inquiry.

3. How CSIS Knows

This chapter focusses on information-gathering by CSIS and some issues it has raised.

Behind Federal Court Warrants

To make use of its most intrusive powers, CSIS requires warrants issued by judges of the Federal Court of Canada. These powers include wiretapping, eavesdropping by microphone, capturing optical images, intercepting recorded communications, searching for documents and paraphernalia, and intercepting mail.

Though not required by law to do so, we read some affidavits sworn in support of warrant applications.

But the affidavits have already been seen by both the Solicitor General and by judges of the Federal Court of Canada before they reach us, so we started to go behind the affidavits to examine the operational files on which they are based.

Because these files are not seen by anyone outside the Service except the Inspector General and us, this provides a distinct second line of defence against unreasonable or unnecessary use by CSIS of its powers.

We found that affidavits were generally factual but, not surprisingly, tended to present the case for the use of intrusive techniques rather than a balanced ledger of pros and cons.

Devil's Advocate. When CSIS asks for a warrant, there is, of course, no advocate for the target.

We are informed that the Solicitor General makes sure, in reviewing warrant applications, that everything being sworn to is an ascertainable fact, not merely a conclusion the investigator has drawn from the facts, and he sends some applications back for amendment before he lets them go to the Federal Court. Indeed, we are informed that he has rejected some requests outright. We welcome his vigilance.

We are also mindful of the role played by the presiding Federal Court judge in each case. While no applications have been turned down by the Court, searching questions have been asked from the bench and conditions designed to protect individual rights have been imposed in the order granting the warrant (see, for example, page 20 of this report).

But the controls now exercised by the Solicitor General and by judges are no stronger than the personal commitment of the people involved. As for us, our review comes after the fact; if there were ever flagrant abuse, we could make our concern known to Parliament, but too late to stop it from taking place.

The Solicitor General, in consultation with CSIS, should consider whether there ought to be a "devil's advocate" at some stage of the procedure—either before the Federal Court or before the Solicitor General himself—to argue the case against the warrant.

This is something that Parliament too might consider when the *CSIS Act* gets its five-year review in 1989.

Basket Clauses. Generally speaking, targets are named in warrants. The location where a warrant can be exercised is specified. "Basket clauses" allow intrusive powers to be used at the same location against unnamed associates of the target, who may be identified only after the warrant is granted. Otherwise CSIS would have to return to the Federal Court for a new warrant each time an associate of the target surfaced.

The Inspector General is currently looking into the issue of who can designate targets under basket clauses in warrants.

We too have a concern about the use of basket clauses and are looking into it. The first question is whether it is acceptable at all. If so, the next question is who within CSIS—or the Ministry of the Solicitor General—should have the power to designate additional targets not named in the warrant.

Counting Them Up

As part of our oversight routine, we have started to compile quarterly statistics on warrants. With our new computer capacity, we can now examine the use of warrants in the aggregate and broken down by types of powers, regions and targets. Aggregate figures for the calendar years 1985 and 1986 are shown in Table 1.

Table 1. New and Renewed Warrants Granted to CSIS, 1985 and 1986

	1985	1986
New warrants	82	94
Warrants renewed	27	11
Total	109	105
Average duration of warrants (days)	173.6	162.2

(Source: CSIS)

Raw data such as we provide here do not permit meaningful comparisons with pre-1985 warrant statistics.

Before the *CSIS Act* took effect on July 16, 1984, warrants for security intelligence investigations were issued under the *Official Secrets Act*. Each of these warrants ordinarily permitted the use of one power against one target.

Warrants issued since then under the *CSIS Act* can be far more sweeping. One of these warrants can authorize the use of many powers against many targets.

Maximum. We are discussing with CSIS the best ways to present the maximum amount of information to the public about warrants and the use of intrusive powers.

We continue to have some concern that aggregate warrant statistics under the *CSIS Act* do not give as accurate a picture of the level of intrusive activities as did the statistics that used to be published under the *Official Secrets Act*.

We get enough information from CSIS to let us develop more revealing statistics ourselves and publish them. But without evidence of abuse, we respect the Service's position that the full story cannot be told without divulging information of significant intelligence value.

This is another issue that Parliament may want to take up when the *CSIS Act* gets its five-year review in 1989.

Other People's Mail

We made a particular study of mail-opening. After the outcry a few years ago over illicit mail-opening by the RCMP, some Canadians were uneasy when CSIS got the legal power to intercept mail, even if this power was subject to the same warrant requirements as any other intrusive activity.

They may have imagined squads of men and women in trench coats and slouch hats, huddled over tea-kettles, steaming open letters to somebody's Aunt Tillie and solemnly recording tidbits of family gossip.

The picture we got was quite different. Apart from the fact that tea-kettles have been overtaken by high-tech methods, very few envelopes had been opened by the end of 1986.

We have reason to expect that mail interception will increase. Only technical difficulties prevented the Service from intercepting the mail of two further targets in 1986. As 1987 began, CSIS held some warrants granting mail-opening powers, ready for use as the need presented itself. A single warrant can cover more than one address.

CSIS says it intends to use this power only when there is reason to suspect that an individual or organization is using the mail to further a threat to national security.

We will continue to monitor mail-opening.

Canada Post is cooperating with CSIS, and a formal memorandum of understanding between the two organizations is being prepared. It will come to us in due course for examination.

We would be pleased to see provisions for cooperation at a less intrusive level than the interception of mail. Tracing, for example. Canada Post is in a position to provide CSIS with lists of the names and addresses that targets correspond with. One issue is whether this, too, should require a warrant.

Emergency Warrants

Before leaving the use of intrusive powers, we raise once more the question of emergency warrants.

An application for a warrant ordinarily originates with an investigator. There is internal review by senior officers and by a formal Warrant Review Committee. Under the *CSIS Act*, each application must be approved by the Solicitor General personally before it goes to a judge of the Federal Court.

Cumbersome as it sounds, this procedure has been streamlined enough to ensure that whenever CSIS has needed a warrant, it has been able to get one in time. Sooner or later, though, an operation is bound to be weakened because a warrant could not be secured quickly enough.

Could This Happen? In our last annual report we outlined a scenario in which CSIS heard at the last minute about a terrorist stopping over briefly in Canada between flights. An instant warrant might be needed so that meetings the terrorist held during the stopover could be monitored. This is the kind of occasion when current procedures may be too slow.

We suggested that the *Act* might be amended so that the Director of CSIS could issue a warrant himself in emergencies, subject to speedy review—within 48 hours, say—by a judge of the Federal Court. We suggested that there should also be an early report to the Solicitor General and to us.

We still believe that special circumstances call for special measures and that some emergency warrant procedures should be written into the *Act*.

To help Parliament when the *Act* gets its five-year review in 1989, we have started to compile statistics on the length of time it takes to obtain warrants. These statistics could help pinpoint any bottlenecks in the system as well as document the need for special measures.

Open Sources

One way that CSIS can limit its reliance on intrusive powers is by mining open sources like scholarly publications and the mass media, both foreign and Canadian.

We are far from satisfied that CSIS takes open sources seriously enough as an alternative to undercover work. The use of open sources remains a pale imitation of what the McDonald Commission envisaged and what we have repeatedly urged for the sake of both effective security intelligence operations and minimum intrusion on personal privacy and freedoms.

We acknowledge that the Service started to create reference sections in regional offices in 1986-87 and that it expanded the Open Information Centre at Headquarters.

This Centre now has a technical services section, a research unit, an Emergency Operations Centre and two reference units. A User Committee was established to help the Centre stay abreast of the Service's real needs, and additional staff was appointed. Some vacancies remain but the key positions have been filled.

Bilingual Service. In particular, we are pleased that the Open Information Centre now employs more bilingual staff and plans an increase to three from one in the number of French-language computer data bases it has access to.

As we note elsewhere in this report (Chapter 8), the Service has lagged badly in giving its Francophone and Anglophone employees equal opportunities to work in their own languages, and every step toward this goal is welcome.

However, services available in French are still far less than those available in English, and we urge all possible speed in carrying out plans to increase the volume of French-language information and services in French. In particular, we hope that a greater use of foreign French-language open media will ensue.

Research. In general, we believe that the Service is not making the most of its opportunities to use open sources.

The research unit gives us great concern. In our last annual report, we noted that the Service had preferred to select researchers from among its "street-wise" intelligence officers, and we suggested that experienced, university-trained professionals would be more appropriate choices.

This point unfortunately needs to be made again. For, although new researchers appointed to this unit are university-educated, they do not have the broad experience in research and government that we think essential.

Furthermore, these researchers are only temporarily assigned to the research unit. They are to be replaced eventually by people with lower job classifications, who will require the appropriate training.

We also believe that better use could be made of the research unit. It now clips items from the media and searches computer data bases for information requested by investigators and analysts.

Researchers do not carry out analyses of their own or even prepare summaries of information on file. This represents a wasted opportunity. It is impossible to resist the suspicion that it reflects the case-oriented approach of police work.

We concur with the McDonald Commission's observation that "security intelligence reports should be less case-oriented; greater attention should be paid to providing government with longer term, more broadly based assessments of security threats facing Canada".*

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 607

Research unit staff are in a unique position to give the Service a global perspective as active researchers—detecting new trends as they take shape, for example.

The Open Information Centre has two ways of handling information. Through its Emergency Operations Centre, it can quickly get information about fast-breaking events reported in the mass media. At a second stage, information is drawn from clippings and computerized data bases.

This is a more comprehensive approach than there has been in the past, but it still begs the question whether research unit staff could be playing a more important analytical role.

Further Needs. Our inquiries revealed that the use made of the Open Information Centre by operating units is not systematically recorded and analysed. We suggest that doing this would be a first step towards seeing where effective use could be increased.

We also encourage the Service to complete its network of regional reference centres as quickly as possible.

Canadian Police Information Centre

Despite some improvement in 1986-87, the Service's access to the Canadian Police Information Centre (CPIC) remains woefully inadequate.

CPIC is a computerized, radio-linked network that gives officers of the RCMP and provincial and municipal police forces instant access to information in three data banks held by the RCMP. These banks cover:

- Vehicle registrations.
- The police records of individuals and outstanding warrants for their arrest.
- Other relevant information about these individuals.

The potential usefulness of CPIC to CSIS is self-evident. Ready access to information on vehicle registrations alone would be invaluable to CSIS surveillants as they follow targets.

But the Service has had to fight every inch of the way to gain even partial access.

The reason—as it is lamely explained to us—is that CPIC was designed to serve "peace officers" and CSIS investigators are not technically "peace officers".

This is nit-picking. When CPIC began, security intelligence fell within the domain of the RCMP, and the people who carried out this work were peace officers. In CSIS, they are civilians without, for example, a peace officer's powers of arrest.

Same Duties. But CSIS investigators have the very same duties and responsibilities that security intelligence investigators had in the RCMP. If CPIC was needed for security intelligence work then, it is needed now.

In both our previous annual reports, we expressed frustration over difficulties CSIS faced in gaining direct access to CPIC. We discussed the issue with the Commissioner of the RCMP personally. Finally, in our last annual report, we urged the Solicitor General, who is responsible for both CSIS and the RCMP, to intervene.

He did so, and the CPIC Advisory Committee has since granted CSIS direct access to the vehicle registrations data bank. But direct access to other banks is limited to counter-terrorism operations only.

When CSIS wants any other CPIC information—the criminal record of a counter-subversion target, for example—it must go to the RCMP, which punches in the request and passes back the read-out.

This entails unnecessary delay, and it fosters an unwarranted notion that CSIS is a junior partner to the RCMP.

Turf Battle. Even the limited direct access CSIS has now is imperfect—to put it mildly. As 1986-87 ended, the RCMP had supplied CSIS with only four CPIC terminals. There was still no terminal at CSIS Headquarters. More were on order, but there is no doubt in our minds that the delay represented continued reluctance to treat CSIS as an equal partner.

Meanwhile, thousands of police officers in quiet suburbs have CPIC terminals mounted under the dashboards of their cruisers, letting them check out teenagers loitering in a parking lot as easily as they could check out the getaway car in a bank robbery.

But no CSIS surveillant in hot pursuit of a suspected terrorist has a similar opportunity to get an instant reading on his quarry.

We see no reason why CSIS should make do with anything less than unlimited access through an adequate number of terminals. This is a classic example of institutions charged with great responsibilities giving priority instead to parochial turf concerns.

Academe and Officialdom

Concerns have been raised in various forums, including the Standing Committee of the House of Commons on Justice and Solicitor General, about fishing expeditions in post-secondary institutions of learning and the use of public servants as regular informants.

Post-Secondary Institutions. Information-gathering at institutions of higher learning must maintain a delicate balance between two social values.

On the one hand there is academic freedom, which implies the opportunity, if not the duty, to express dissent peacefully, without fear of harassment. Many times in history, one generation's radicalism has become the next generation's pillar of social order. Democracy itself has had its times of disrepute.

On the other hand, CSIS must be able to pursue its investigations wherever hostile intelligence officers or their agents, terrorists or subversives lead it.

We have now confirmed that the Solicitor General's instructions and policy on campus operations by CSIS conform to the position established for the RCMP and agreed to by the Canadian Association of University Teachers in 1963, that:

> There is at present no general RCMP surveillance on university campuses. The RCMP does, in the discharge of its security responsibilities, go to the universities as required for information on people seeking employment in the public service or where there are definite indications that individuals may be involved in espionage or subversive activities.

The activities in question are now those defined by section 2 of the *CSIS Act* as "threats to the security of Canada".

The decision whether to carry out investigative activities on campus is further limited by a ministerial directive of June 8, 1984. It provides that investigations should occur only where there are "objective indications that individuals may be involved in activities prejudicial to Canada", and it requires ministerial approval for certain kinds of investigation.

Public Servants as Sources. Concerns have been raised about the use of federal government employees as sources because of the pressure they might feel to cooperate with CSIS in order to protect their jobs.

A secret directive issued by the Solicitor General lays down general principles governing the use of federal employees as sources.

Inter-Organizational Arrangements in Canada

Apart from the issue of undercover sources in federal jobs, CSIS needs access to records held by police forces and other government agencies—federal, provincial, local and foreign—to do its job effectively and efficiently.

Perhaps CSIS's most important partner is the RCMP. Indeed, the relationship has so many ramifications that we defer our discussion of it to a special section in Chapter 5.

Formal arrangements between CSIS and other bodies require the prior approval of the Solicitor General, and we review them after the fact.

Federal Departments. In 1986-87, we got copies of memoranda of understanding with three federal departments, giving CSIS access to personal information as permitted under paragraph 8(2)(*e*) of the *Privacy Act*—that is, information required to enforce any law or carry out a lawful investigation.

The departments are Revenue Canada (Customs and Excise), the Department of the Secretary of State and the Canada Employment and Immigration Commission. There are two agreements with the Canada Employment and Immigration Commission.

This brought the total number of agreements with federal departments and agencies to six; there were already agreements with Canada Post* and the Department of External Affairs.

We are satisfied that these agreements adequately protect personal privacy while providing CSIS with enough access to do its job.

Provinces and Police. Copies of five memoranda of understanding providing for liaison and exchanges of information with provincial government departments and with police forces other than the RCMP came to us during 1986-87.

These agreements are with British Columbia, Alberta, Ontario, Prince Edward Island and Nova Scotia.

We found them unobjectionable from the privacy point of view.

But we noted with some concern that they do not appear to be binding. We hope they will not prove to be the seedbed of future problems if CSIS needs information that the provinces or police are, for any reason of their own, reluctant to give.

We also take the occasion to suggest that CSIS keep full and accurate records of all contacts under these memoranda.

And we urge high priority for the negotiation of agreements with the remaining provinces to ensure a smooth, rapid flow of information both ways when it is needed.

Foreign Arrangements

Arrangements with foreign governments generally cover exchanges of information to meet three needs—vetting applications for visas and immigration, carrying out security clearances and, finally, protecting the respective national interests of Canada and the other country.

CSIS also has some arrangements with sister security and intelligence agencies for cooperation in such matters as professional training.

In 1986-87, we got copies of five new and revised agreements with foreign governments. We also saw copies of the ministerial direction authorizing each agreement. All were in order.

There have been concerns that CSIS did not clearly distinguish between foreign liaison arrangements that were merely desirable and those that were strictly necessary.

---

* Earlier, we indicated that an agreement is still being worked out with Canada Post to govern mail-opening operations. The agreement referred to here deals with Canada Post's own files.

We are of the opinion, supported by independent legal advice, that the "strictly necessary" rule found in the *CSIS Act* (section 12) does not apply to the conclusion of agreements with foreign governments. It is sufficient that such agreements be conducive to the protection of national security. But we are pleased, nonetheless, that the Solicitor General has sought clearer statements of necessity from CSIS in its proposals for new arrangements.

So that we can monitor arrangements with foreign governments more knowledgably in future, we have asked the Solicitor General to start sending us copies of the letters in which the Secretary of State for External Affairs comments on each arrangement as it is proposed.

Two continuing foreign liaison issues call for particular comment—the legacy of arrangements negotiated by the RCMP and, second, the position of CSIS liaison officers in certain Canadian missions abroad.

The RCMP Legacy. Early in 1985, we received from CSIS thousands of pages that it inherited from the former RCMP Security Service, setting out existing arrangements with foreign governments and their agencies. In our previous annual reports, we recommended that these arrangements be reviewed in light of the new *CSIS Act* and renegotiated.

Since then, a new consolidation of foreign arrangements has been prepared, examined by the Department of External Affairs and approved by the Solicitor General.

We have come to the conclusion, supported by independent legal counsel, that the transition provisions of the *CSIS Act* are broad enough to validate foreign arrangements originally entered into by the RCMP, making renegotiation unnecessary on purely legal grounds.

In consolidation, CSIS also let some arrangements lapse. This was sensible; some that were appropriate for a police force like the RCMP (whose members have, for example, powers of arrest) were inappropriate for a civilian security and intelligence service (whose members do not).

Liaison Officers. CSIS has security liaison officers in some Canadian missions abroad, responsible for providing timely and relevant information and assessments on security matters to the Service and to the authorities of the host countries.

We have examined the role these officers play and find it consistent with the *CSIS Act*.

But we found some confusion about the respective responsibilities of CSIS's liaison officers and the RCMP liaison officers who are also posted to some missions. We will return to this subject in our general discussion of CSIS-RCMP relations (page 29).

Unlawful Acts

The Director reported, under the *CSIS Act* (section 20), that an employee may have overstepped the law on the job by failing, on two separate occasions, to obtain routine signa-

tures from a supervisor on documents authorizing certain acts. The employee has been reprimanded and is now well aware of the requirement for the signature. We agree that no charges are warranted.

There have also been a small number of incidents in which CSIS employees have been investigated by management for misbehaviour off the job. These investigations led to dismissal or resignation. Since they are not related to the work of the Service, we regard them as a matter of personnel administration.

Solicitor-Client Privilege. However, there was a serious breach, which the Director did not report as such, when records of solicitor-client communications were retained in three of the Service's five regions for about a year, in defiance of conditions written into the relevant warrants by Federal Court judges.

The problem arose when new instructions from Headquarters on the retention of records generally were misunderstood, and it was swiftly corrected when it came to light. Because of their privileged nature, the records had been sealed, and they are being destroyed as required by the warrants.

Gap. In the short term, no material harm was done. We have read the report of the Inspector General who, after a thorough investigation, came to the same conclusion. However, this situation highlights a gap in the *CSIS Act*; unlike the *Criminal Code*, it affords no protection to solicitor-client communications.

On the face of it, this is disturbing. People should be free to discuss their legal affairs in complete frankness with their lawyers, confident that what they say will not be disclosed without their consent. This is the essence of solicitor-client privilege.

So we looked into this matter closely and discussed it on three separate occasions with CSIS at the deputy director level.

As a result of media reports,* we also made inquiries about a specific case of intercepted communications between a lawyer and his client. We were satisfied that there were genuine security concerns to justify interception in this case. We also noted that the information gained was not passed on to any other agency.

Delicate Balance. This left us with the overall issue to consider. As in so many other areas of security intelligence, there is a delicate balance to be maintained.

Without reference to any particular incident, it is easy to imagine circumstances in which interceptions would be justified—when the lawyer appeared to be a co-conspirator with the "client" against the national interest or when a lawyer acted as a message centre for conspirators. Not even under the *Criminal Code* is the lawyer's gown roomy enough to shelter communications that concern illegal acts involving the solicitor.

* Notably in *The Globe and Mail*, Toronto, January 8, 1987.

Federal Court judges have made a practice of writing particular protections for privileged solicitor-client communications into warrants, as follows:

- Prohibiting the interception of communications at the office or residence of a solicitor or at any other place ordinarily used by a solicitor for the purpose of consultation with clients. (This parallels the protection found in the *Criminal Code*.)
- Restricting the interception of calls made between the target and the solicitor (or the solicitor's employee) to calls that the Director or a regional director general determine are related to the threat specified in the warrant.

Present Arrangements. CSIS has procedures for giving effect to these conditions. When a record is made of communications between a solicitor and the client, it is submitted to the Director or a regional director general. If he determines that the communication does not further a threat to the security of Canada, all records of the communication are destroyed and no disclosure is made.

Except as we have explained above, we believe that these procedures are respected. But we are not satisfied that this is enough.

One concern is that, like the Solicitor General's review of warrant applications and our review of the operational files behind them, these safeguards rely on individual commitment—that of Federal Court judges to keep writing them into warrants. Unless the safeguards are written into law, that could change at any time.

This is a further issue that Parliament may want to consider when the *CSIS Act* gets its five-year review.

4. What CSIS Knows

Having examined in the last chapter how CSIS gets information, we turn now to its management of information. Is CSIS keeping unnecessary confidential information, especially about individual Canadians? How is the information that it accumulates used? In this chapter we focus on the first question, leaving the second to be dealt with in Chapter 5.

Legal Limits

The *CSIS Act* sets two important limits on the collection of information, as follows:

- The information must be related to "threats to the security of Canada" (section 2).
- Such information may be collected to the extent that is "strictly necessary" to deal with activities that can reasonably be suspected of being threats (section 12).

For easy reference, it may be worth quoting section 2's definition in full here. It says that the term "threats to the security of Canada" includes:

> (*a*) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (*b*) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (*c*) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state,
>
> (*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,
>
> but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).

Inherited Information

Against this background there are serious legal as well as ethical questions to be asked about information in operational files that CSIS inherited from the RCMP Security Service.

Some of it was gathered during the unhappy period documented by the McDonald and Keable Commissions, when some investigators let their genuine concern for national security run away with their appreciation of privacy and the right to engage in democratic dissent. We are also thinking of information dating back to the heyday of protest and the so-called New Left in the 1960s.

No one knows everything that is in these files, because they have not all been systematically reviewed. But, in light of the McDonald and Keable findings, some concern is reasonable: Does all this information meet section 2's definition of a threat to the security of Canada? Is it all still strictly necessary, as required by section 12?

If the answer to either of these questions is No, then more questions arise. Does CSIS have legal authority to keep unnecessary or irrelevant information on file? Might any initiative based on such information be subject to challenge before the courts?

CSIS has resisted our urgings that it review all these files and weed out material that does not meet the requirements of sections 2 and 12. There are, we admit, some real difficulties.

Moratorium. In the short term there is the moratorium placed on file destruction following the Deschênes Commission's discovery that old immigration files it needed in its investigation of alleged war criminals had been routinely destroyed. We return to the question of out-of-date CSIS files in a moment.

Even if the moratorium were lifted, it would be a gargantuan task to go through these files one by one, getting rid of any inappropriate information.

At another level, we must recognize too that gathering and looking for threatening patterns in apparently innocent bits and scraps of information is the business CSIS is in.

Anyway, said CSIS, it should be enough that inappropriate information found in these files not be used; that is what our Committee is for—to blow the whistle if limits like the "strictly necessary" rule are overstepped.

We don't shrink from our responsibility to monitor the Service's use of information. But we also face a problem of scale; we can hardly watch every move of every member of the Service. And we find it hard to imagine that irrelevant information, even if it is not technically "used", would not at least colour the approach of an investigator or analyst who saw it.

So we would still like to see these files systematically weeded. The task could be reduced to manageable proportions if it were done progressively, on a pre-determined schedule over a period of years.

We were pleased to learn in the course of the year that the Solicitor General shares our concerns and has asked CSIS to develop file retention standards in conformity with sections 2 and 12 of the *CSIS Act*.

Retirement of Old Files

This brings us back to the question of retiring and destroying entire files that have outlived their usefulness—a concern we inherited from the McDonald Commission.*

As a result of the McDonald Commission's observations, the RCMP Security Service and the Dominion Archivist—who is responsible for assessing and approving proposals to retain or destroy federal records—developed disposal schedules for inactive files.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 521

In the late 1970s, there was a major disposal of files that had been opened before 1973. Then between July, 1984, when CSIS took over from the Security Service, and February, 1985, when the moratorium described above came into effect, some 77,800 files with no security intelligence value were destroyed after review.

Today, more than 67,000 files are ready for destruction once the moratorium ends.

We are keeping an eye on this issue and have asked for copies of the disposal schedules. We note that government policy calls for a review of such schedules every five years, and we were encouraged to learn that CSIS launched such a review with the Dominion Archivist in December, 1986.

Foreign Intelligence

Another issue became apparent when we examined the flow of information in one operational branch of CSIS.

It seemed to us that information supplied by friendly foreign intelligence services might too easily be accepted by CSIS at face value; it may not be getting the same critical scrutiny as information from Canadian sources.

Indeed, we sensed that CSIS might be too quick to accept the foreign policy underpinnings of this information instead of recasting it in terms of Canadian policy (see, for example, page 37 of this report). Canada has its own national interests, distinct from the interests of any other nation.

The McDonald Commission pointed out the danger of adopting the "outlook and opinions of a foreign agency, especially an agency which has come to be depended upon heavily".* The warning remains timely.

Due Weight. The *CSIS Act* requires the Service to consult with the Department of External Affairs on various aspects of international relations (paragraphs 17(1)(*b*) and 19(2)(*b*). We encourage closer collaboration between CSIS and this Department in the assessment of international events and the conduct of CSIS's activities to ensure that Canadian foreign policy gets its due weight.

The McDonald Commission also noted, incidentally, that greater use of open information could be a bulwark against excessive dependence on one or more foreign agencies. This supports our contention that CSIS should be making greater use of open sources (see page 12 of this report).

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 632

Incidental Information

In 1986, CSIS developed new policy for dealing with information acquired inadvertently although it has nothing to do with national security concerns. CSIS defines two categories of such information—"spin-off" and "incidental".

Spin-offs are information with potential use in criminal law enforcement, national defence, the conduct of external relations or the general pursuit of the national interest. We deal with it in the next chapter of this report.

Incidental information is everything else that is not necessary to national security. Such information is—quite properly—destroyed.

There are some kinds of information that CSIS should clearly be deaf to—and mute about. For example, it must never interfere in the democratic process by letting the government know about anything like the electoral strategy of a legitimate opposition party. We believe that it has never done so.

5. What CSIS Does

The bottom line is how CSIS's information is used. Some issues this raises are the subjects of this chapter. Cooperation with the police is one major use that can be made of CSIS information, so operational relationships with the RCMP are also dealt with here.

Spin-Off Information

We ended the last chapter with a discussion of "incidental information" that is destroyed because it is not useful either for national security purposes or for criminal law enforcement, national defence, the conduct of international relations or otherwise in the national interest.

Unsolicited information that could be useful for one of these non-security purposes is termed "spin-off" information. Under the *CSIS Act* (section 19) it can be passed on to the appropriate authorities.

If CSIS were firing off advisories in all directions with spin-off information, we might worry that it was casting its net wider than "strictly necessary" (section 12 of the *CSIS Act*) and concerning itself with more than threats to the security of Canada.

In fact, our concern is that the Service seems too cautious in this regard.

CSIS in Court

The Service's jealousy of its secrets has been spotlighted for the public more than once as its officials have interrupted trials and cut off questioning of their colleagues, citing the *Canada Evidence Act*. Subsection 36.1(1) of this *Act* provides that:

> A Minister of the Crown in right of Canada or other person interested may object to the disclosure of information before a court, person or body with jurisdiction to compel the production of information by certifying orally or in writing to the court, person or body that the information should not be disclosed on the grounds of a specified public interest.

Section 36.2 provides for the hearing of objections in the Federal Court of Canada when it is alleged that disclosure "would be injurious to international relations or defence or security" and also for appeals.

Headlines like "Spywork: How it can close down a court" (*Toronto Star*, June 21, 1986) and "Gag order needs no reasons" (*Ottawa Citizen*, June 7, 1986) have been the result of CSIS interventions under the *Canada Evidence Act*.

This is not an unexpected issue. Keeping sources and "tradecraft" secret is a preoccupation of all security and intelligence services. Protecting human sources is a special concern. An informant whose cover is blown may not be useful any more. And potential sources are bound to shun a service that does not protect them from exposure and its consequences.

All Relevant Evidence. Nonetheless, we feel that means must be found to ensure that all relevant evidence is heard by the courts—if not by the public—in criminal cases. For one thing, CSIS evidence might tend to show the innocence of the accused; in such a case, silence seems to weaken the fundamental principle that before our courts a person is innocent until proven guilty.

We note that the *Criminal Code* makes provision for excluding the public from court rooms for reasons of "public morals, the maintenance of order or the proper administration of justice" (section 442).

Would it help if "national security" were added to the list? The difficulty is that this would not exclude the accused, who might have a clear interest in such matters as identifying informants and learning CSIS procedures.

So there is no easy answer. It is another issue that Parliament may wish to take up when the *CSIS Act* gets its five-year review in 1989.

Assistance to Police

This leads us into the whole issue of CSIS relations with the police. For CSIS is tight-lipped not only in court. Because of its concern for the secrecy of its operations, it has at times withheld information from the police.

We share the view of the McDonald Commission* that CSIS ordinarily has a duty to tell the police what it knows about criminal activities. If, for example, a surveillant parked in the shadows sees someone stealthily cutting glass out of a jewelry store window, looking for all the world like a burglar at work, the police should ordinarily be called in. This is permitted under paragraph 19(2)(*a*) of the *CSIS Act*.

We acknowledge that there are exceptions—when a police investigation, and perhaps evidence at a subsequent trial, would irremediably compromise a vital security operation. For example, if the arrival of a police car would prompt important targets to move to a new location unknown to the Service.

Regional Directors General decide whether information about criminal activities should be passed on to the police. Guidelines are set out in an Operational Bulletin issued under the authority of the Director of CSIS.

On Its Merits. What the rules boil down to is that each case is considered on its merits in light of the seriousness of the supposed offence, the protection of CSIS sources and the potential for damage to CSIS's operational capability if its involvement in reporting the offence became known. The Service is looking into the need for more formal guidelines.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), page 605

Our preference is already clear. We are content to see decisions made by the regional directors general. But we believe that the criteria should be set in a new ministerial directive, to shelter them from any arbitrary change that CSIS itself might make in future.

Relations with the RCMP

While senior managers in both CSIS and the RCMP seem increasingly comfortable within their respective boundaries, it has obviously been harder to plot the line inch by inch in the field.

The term "healthy tension" has been used to describe the situation, but we think it would be even healthier if it were a little less tense. We are encouraged, though, that problems are recognized and that steps are being taken to deal with them.

The Solicitor General has provided us with a copy of a memorandum of understanding between the RCMP and CSIS, consolidating a number of arrangements for cooperation and for sharing services and administration.

He informed us that he had deferred approval of chapters on CPIC and information sharing. We support this decision. CPIC we have already discussed (page 14 of this report). As for information sharing, we have written to the Solicitor General to voice our concerns that there may be duplication of effort between CSIS and the Crime Intelligence Branch of the RCMP.

With these reservations, the memorandum provides a firm base for relations that are smoother because they are clearly defined in a number of mundane areas like accommodations, air services, multilingual translation services, pay administration, photographic services, printing and the use of secure telecommunications devices and electronic data processing.

Liaison Officers. The Solicitor General established an exchange of liaison officers between the CSIS and RCMP counter-terrorism programs in the latter part of 1986.

Counter-terrorism is where the CSIS and RCMP mandates touch most closely and are most likely to grate. There are, as the Director of CSIS, among others, has pointed out,* two needs in this field.

There is an intelligence need directed at predicting and sidetracking incidents—the CSIS domain. And a law enforcement need directed at apprehending criminals and assembling sufficient evidence to convict them—the RCMP domain.

At the stage when a criminal conspiracy is afoot, before an incident has occurred, the two domains overlap. CSIS-RCMP cooperation is plainly essential. The *CSIS Act* provides for

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, December 11, 1986

this overlap by setting out quite clearly the intelligence responsibilities of CSIS and the law enforcement responsibilities of the RCMP (sections 12 and 61).

Airport Security Alert

Unfortunately, what we actually found in a case study of one counter-terrorism operation—the "airport security alert"—was turf battles and distrust.

The story began in December, 1985, when police were tipped to an alleged Libyan plot to place a bomb on a commercial airline flight originating in Ottawa.

Security precautions were subsequently increased at major airports, at considerable cost to the taxpayer and considerable inconvenience—to say nothing of anxiety—to travellers. Furthermore, the threat diverted public safety personnel from other important duties and disrupted routine police investigations.

Whether it was because the information was frivolous or because early exposure of the conspiracy and efforts to head it off led to its cancellation, no explosion occurred. Airport security precautions returned to normal.

Case Study. Fresh from the Air India and Narita Airport disasters of 1985, Canadians heaved a sigh of relief and went on with their business. We too went on with our business and seized the opportunity to make a thorough case study of how CSIS and police forces work together in an anti-terror operation.

This case was a good example of where counter-terrorism, criminal investigation and security intelligence all come together, requiring the cooperation of various players and the need for working closely within their roles and functions.

We are not, of course, at liberty to publish our full report. Besides security considerations, some of our informants were promised confidentiality in return for their cooperation. The RCMP and the Ottawa City Police, which were responsible for the criminal investigation, are not answerable to us. But we are grateful to them, as well as to CSIS, for their unstinting help in this inquiry.

However, we have made a report to the Solicitor General with our conclusions and recommendations.

Reticence. It was not clear to us that CSIS was a full participant in the *ad hoc* task force that took shape to track down the alleged conspirators. It quickly became very obvious that the flow of information between CSIS and the police could have been better.

The reticence worked both ways. The police, who had the original tip, waited six days before calling on CSIS for help, for example. We had the impression that the RCMP, in particular, felt that this was exclusively a police operation.

On the other hand, CSIS missed an opportunity to counter that feeling when it did not take up an invitation to assist in some surveillance.

Guidelines. Indeed, we discovered that CSIS and the RCMP had yet to completely mesh their mandates in counter-terrorism. While the exchange of liaison officers mentioned above is a valuable step, we see a need for formal operational procedures. Among issues that procedures should deal with are:

- Limits that can be put on the use of shared information.
- How responsibility for surveillance duties should be shared.

Meanwhile, we recommended that the Ministry of the Solicitor General carefully monitor the liaison arrangement and keep the Solicitor General informed of progress.

We also recommended ministerial direction to encourage appropriate sharing of information in the investigation of terrorist activities that require the attention of both CSIS and the RCMP, even on such sensitive matters as the identity of sources, recognizing that intelligence ultimately required for court proceedings should be provided in a way that protects future intelligence initiatives.

Public Relations. One finding was that local police forces do not seem fully aware of CSIS's role. So we have recommended that CSIS undertake a public relations exercise to provide law enforcement organizations with information on its mandate, role and activities, reminding them that it is separate from the RCMP.

This would encourage local police forces to deal with CSIS directly as well as with the RCMP in meeting terrorist threats.

In a similar vein, we recommended high priority for completion of the network of mutual cooperation agreements between CSIS and provinces (see page 17). None was in effect at the time of the airport security alert.

Perfect airport security at all times is not possible; there will always be ways to disrupt the peace that travellers in Canada generally enjoy. This makes it doubly important to ensure unreserved cooperation of the kind that the Solicitor General has moved to bring about between the RCMP and the Service.

Foreign Liaison Officers

Progress is being made outside the country, at Canadian missions where CSIS and the RCMP both have liaison officers. It has been agreed that CSIS now vets visa applications—as we believe it should under the letter and the spirit of section 14 of the *CSIS Act*.

It should be noted that CSIS and the RCMP have mutual assistance arrangements in posts where only one or the other has a liaison officer. This seems to work well.

Persona Non Grata

CSIS did make good use of its findings to identify foreign agents operating in Canada under the cloak of diplomatic immunity.

As a result of information it passed on to the Department of External Affairs, two members of foreign missions were declared *persona non grata* in 1986-87 and were sent home. Six more were voluntarily recalled home from Canada.

The Public Interest

Statutory rules govern disclosure to a minister other than the Solicitor General or, in specified circumstances, the Secretary of State for External Affairs or the Minister of National Defence, and disclosure to a public servant when it is "essential in the public interest and that interest clearly outweighs any invasion of privacy that could result" (paragraph 19(2)(*d*) of the *CSIS Act*).

The consent of the Solicitor General is required and, under subsection 19(3), the Director must make a report to us afterwards.

We received no reports on such disclosures in 1986-87.

Front Organizations

The *CSIS Act* does not contemplate disclosure to voluntary organizations or their members in case of infiltration by persons who may want to use them for purposes that could represent a threat to the security of Canada.

We raised this issue in last year's annual report, pointing out that loyal Canadians who belong to infiltrated groups or groups threatened with infiltration deserve to be alerted if some means can be found of communicating appropriate information.

Was there also some way, we asked, in which individuals who join a "front organization"* because they support its overt aims could be warned of its covert objectives?

Since then we have learned in CSIS briefings that hostile foreign intelligence services have, indeed, infiltrated some organizations and that substantial funding from foreign sources has been detected.

If CSIS were to publish such information, it would, in the process, reveal carefully guarded sources of information. It would be naive to suggest that those being watched do not know it. But publication of any detail could compromise surveillance.

---

* A definition we suggested was: "An outwardly independent organization whose promotion of idealistic, humanitarian and non-partisan political issues serves to obscure its covert objective of promoting public support for policies and initiatives of the organization or foreign power by which it is controlled". We added that "membership in a front organization should not be construed as knowledge of, agreement with, support of or adherence to the organization's covert objectives".

We do not have any easy answers to offer. As we did last year, we simply suggest that this is a problem Parliament might want to address when the time comes to review the *CSIS Act*.

A Vigilant Canadian. Meantime, we were heartened by one result of our reference to this matter last year.

After reading our annual report reference, a person deeply committed to a cause undertook to subject a front organization executive to vigorous and penetrating questioning. The executive finally tacitly acknowledged the real purpose of the organization, which had little to do with that cause.

Our reader promptly withdrew support and persuaded other, like-minded persons to do the same.

If we could count on equal vigilance on the part of all Canadians, we could abandon the search for a means through which members of front organizations and organizations subject to infiltration could be warned.

6. Counter-Subversion Operations

Counter-intelligence and counter-terrorism offer little room for disagreement. A given foreign nation either spies on us or it does not. No exception can be taken to counter-intelligence aimed at protecting our secrets from those that do.

Similarly, there is no place for terrorism in a country like ours with well-entrenched democratic means for gaining and using power. Any of us could be the innocent victim of a terrorist act. Clearly, those who would use violence to reach their political goals must be detected and stopped.

Counter-subversion is different. The right of peaceful dissent is the bedrock of democracy. Yet there are a few Canadians who proclaim their belief in the need for violent revolution. And even peaceful dissent may be secretly perverted by foreign powers whose goals are not the goals of most Canadians.

Grey Zones. At what point does dissent make an individual or an organization a legitimate target for the Counter-Subversion Branch of CSIS? How much talking about violence does it take to raise a real threat of violent acts? When does contact with foreign powers become detrimental to the interests of Canada?

Many such questions can be asked, and the answers turn up rich soil where honest disagreement can flourish. This is why we made counter-subversion the subject of our first branch-wide study of CSIS.

We are restricted in what we can say, of course. However, we can describe the research we undertook and set out some findings and recommendations.

Our criticisms of the system are not, we stress, directed at the men and women who carry out counter-subversion programs. We were impressed by the dedication and talent brought by both management and staff to their work and by the real difficulties they face in applying the *CSIS Act* in this grey zone.

Nonetheless, it is our duty to flag the concerns that our study gave us and to encourage CSIS to correct weaknesses in the system.

Principles and Law

As our standard, we adopted five basic principles from the McDonald Commission,* as follows:

- The "rule of law" is paramount.
- The means of investigation must be proportionate to the gravity of the threat and the probability of its realization.
- The need for given investigative techniques must be weighed against the damage they might do to personal freedom and privacy or to valued social institutions.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), pages 513-514

- The more intrusive the technique, the higher the authority that must be required to approve its use.
- Except in emergencies, less intrusive techniques must be preferred to more intrusive techniques.

We were also guided, of course, by the *CSIS Act*, notably:

- The definition of "threats to the security of Canada" (section 2), in which Parliament was careful to exclude "lawful advocacy, protest or dissent". (The text of the definition can be consulted on page 21 of this report.)
- The requirement (section 12) that information be gathered only "to the extent that it is strictly necessary".

How We Proceeded

In our study, we examined policy and operational procedures to determine whether they met statutory requirements, and we discussed these procedures with senior CSIS managers.

We covered planning and accountability processes, the resources and investigative tools used in counter-subversion (compared with the resources and tools used by the Counter-Intelligence and Counter-Terrorism Branches), the number of paid sources, the amounts such sources are paid, targeting procedures, the number and nature of files opened on Canadians, and the amount of information disseminated to the Canadian and foreign governments about Canadians.

We also examined actual cases to see how policies and procedures are put into practice.

All of this was done against the background of McDonald Commission findings and an examination that we made of reform of the FBI (Federal Bureau of Investigations) in the United States in the mid-1970s. We met in Washington with officials of the FBI and with senior staff of the Permanent Select Committee of the House of Representatives on Intelligence and the Senate Select Committee on Intelligence.

Transition

We reviewed transitional activities—efforts to orient staff and to change policy and regulations in 1984, when the *CSIS Act* came into force and CSIS took over security and intelligence responsibilities from the RCMP Security Service.

More than two years after the switchover, the review of procedures remained incomplete. The Operational Manual was still outdated and even, at some points, contrary to the spirit of the *Act*.

This was disturbing, but CSIS is aware of the problem and is putting the manual through a drastic revision. We look forward to examining the new version as soon as possible.

We learned that all Security Service investigations reviewed in 1984 were continued by CSIS—although sometimes under justifications rewritten to ensure conformity with the new *CSIS Act*. Two investigations reviewed only at a later stage were dropped.

Resources

Counter-subversion gets a relatively small share of CSIS resources. Testifying before the Standing Committee of the House of Commons on Justice and Solicitor General last year,* the Director set the figure at "under five per cent".

While we appreciate the basis on which the Director spoke, we think that "10 per cent, or slightly more, of operational resources" is a more realistic statement. Nonetheless, this is a relatively small proportion.

During our study, we found some frustration among CSIS investigators who felt that counter-subversion was the neglected step-sister of the CSIS family, with inadequate resources compared with counter-intelligence and counter-terrorism. Indeed, we found that counter-subversion sometimes seemed to be used as a personnel pool that could be drawn on to meet urgent needs in other operational branches. The Counter-Subversion Branch is taking steps to improve morale.

Human Sources

A separate Human Sources Branch serves all operational branches. It focusses mainly on paid sources. It seeks, for example, to ensure that they are reliable. It also has rules about what paid sources can and cannot be asked to do. But it does not do the same for regular unpaid sources.

There is no central control of "tasking"—that is, telling sources, both paid and unpaid, exactly what targets to monitor and what kind of information is wanted. Tasking is the responsibility of individual operational branches.

Targeting

The choice of primary targets for investigation is overseen by a Target Approval and Review Committee (TARC) composed of senior CSIS managers, advised by counsel. Like the Human Sources Branch, it serves all the operational branches.

---

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, December 11, 1986

TARC authorizes targeting for specified periods of time, so it deals with renewals as well as with new targets.

It makes its decisions after examining Subject Evaluation Reports (SERs) prepared by investigators.

Groups are targeted on the basis of section 2 of the *CSIS Act*. In counter-subversion, undue foreign influence and the potential for violence are the criteria most often used.

Individuals can also be targeted on the basis of section 2. But most individuals become targets automatically because of their relationship with a targeted group.

Not every subject who is targeted is actively investigated. The decision to investigate particular individuals is made by regional or branch managers based on the apparent threat, the information called for in CSIS's annual plan, and the availability of resources.

Some targeted individuals are investigated actively (a warrant may be sought to tap their telephones, for example) and some passively (in some cases amounting to no more than the accumulation of items about them from the press).

As anyone might guess, leaders of targeted groups are more likely to be watched closely than are rank-and-file members who, in turn, are more likely to be watched closely than are sympathizers who are not members. The term "leaders" includes influential mentors as well as people who hold office in the targeted group.

The categories of individual to be investigated because of their relationship with a targeted group are chosen by TARC.

But there is also another class of targets, composed of everyone in regular contact with a person already targeted for active investigation by TARC. These second-stage targets are identified in the field and do not come to TARC's attention at all.

For a number of reasons, we are concerned that the counter-subversion program casts its net too widely.

Targeting by Category. One way of looking at the TARC process is as we have described it above—that is, targeting entire categories of persons. Another is that individuals are targeted without reference to the actual threats, if any, that they personally pose to the security of Canada.

We find this insufficiently precise. Some groups under covert foreign influence, for example, may include only a few members who are aware of that influence. Even in groups with radical visions of the future, violence may be the preferred means for only a few members. It is not self-evident that all the officers of front groups would necessarily know these groups' covert agendas or undertake activities damaging to the security of Canada.

We think it would be more useful to explore means for warning such people of the organizations' real purposes (see page 30 of this report).

Our concern extends even more strongly to the people we have described above as second-stage targets—those identified merely because of repeated contact with a targeted individual.

Potential Harm. From what we have said about targeting by category, it follows that the present process takes insufficient account of potential harm to the principles of personal freedom and privacy.

Nor does the targeting process concern itself with the harm that can be done to valued social institutions if, for example, surveillance frightens members away from voluntary associations that would otherwise give them opportunities to promote legitimate causes and to devote their talents and resources to charitable purposes.

We urge that SERs always include a balanced discussion—pro and con—of the damage that investigation could do to individual freedoms and privacy and to the integrity of social institutions. The SERs that we saw were silent on these issues.

What Constitutes a Threat? Some of the threats described by CSIS are clear-cut; all loyal Canadians would agree that they deserve the Service's unremitting attention. But some left us perplexed.

One SER, for example, spoke of a certain organization's "attack on the anti-communist, pro-U.S. government of El Salvador ... in direct support of ... policy objectives to ... blunt American foreign policy initiatives". We cannot agree that a non-violent attack on U.S. foreign policy is necessarily a threat to the security of Canada.

On the other hand, there seems to have been minimal CSIS interest in fund-raising inside Canada for the Contra rebels in Nicaragua—although this seems to meet section 2's criterion of "activities within ... Canada ... in support of the ... use of acts of serious violence against persons or property for the purpose of achieving a political objective within ... a foreign state".

This contrast lends weight to our concern (see page 23 of this report) that CSIS may too readily accept the foreign policy objectives of our allies as its own and neglect Canadian foreign policy.

Magnitude of the Threats. CSIS seems to share our view that Canada faces minimal threats from many of the groups targeted by the Counter-Subversion Branch.

We recognize the real threats posed by a few. However, CSIS is expending money and effort on too many counter-subversion targets and it is intruding on the lives and activities of too many Canadians in this area.

Recommendations. We have already suggested that SERs always include a discussion of the harm that investigation could do to individual freedoms and privacy and to the integrity of social institutions.

In addition, TARC should reconsider its practice of targeting entire categories of people and examine the possibility of treating individuals as individuals. SERs would then have to document the need for investigation of individuals one by one.

We suggest that SERs also include explicit discussions of (a) the magnitude of the threat and (b) its imminence, (c) the need for the type of investigation envisioned compared with less intrusive alternatives and (d) the goals of investigation.

They should rely less on isolated incidents and more on a coherent argument for the targeting decision that TARC is asked to make.

In the same vein, we would also be more comfortable if greater efforts were made to ensure that all applications for warrants noted evidence that did not support the use of intrusive powers as well as evidence that did (see page 9 of this report).

CSIS should maintain a complete and up-to-date index of individuals subject to investigative authorization, instead of the partial index that exists now.

Files on Individuals

Files are opened on targeted individuals and organizations. We were unable to determine the precise number of files opened as a result of counter-subversion operations as they are not segregated from counter-intelligence and counter-terrorism files.

According to the best information we have been able to obtain, the Counter-Subversion Branch probably has more than 30,000 files on individuals—how many more, no one knows. This is a matter of some concern to us. We don't know and we can't find out without a manual examination of thousands of files.

Only a small proportion of the people with files are under active investigation.

To further place the 30,000 figure in context, CSIS as a whole holds more than 600,000 files on individuals.

(It opened 112,000 such files in 1986-87. These include administrative files on, for example, the Service's own employees, as well as security assessment and immigration-related files, which turn over rapidly.)

Despite efforts in the early 1980s to purge files with little or no intelligence value, the number of files on individuals in the counter-subversion area seems to have remained relatively constant compared with the number held by CSIS's predecessor, the RCMP Security Service.

Old Files. Many of the files now held were opened when security intelligence was the responsibility of the RCMP Security Service, before there was a statutory definition of "threats to the security of Canada" (section 2 of the *CSIS Act*) or the "strictly necessary" rule (section 12) was laid down.

We have already made it clear in this report (page 21) that we think CSIS should review its files on individuals and remove information that does not meet the standards of sections 2 and 12.

We also suggest that detailed criteria be developed for opening files on individuals and groups and that the implementation of these criteria be reviewed periodically.

Dissemination of Information

When we asked CSIS how much information was provided to Canadian and foreign government agencies, we were told that the management information system could not readily identify such items. Each file shows what information went to whom. But there is no coding that lets aggregate figures be determined without a file-by-file search.

This gap could make it more difficult for us to meet our oversight duties for sections 17 and 19 of the *CSIS Act*, which deal with the exchange of information.

We urge that the management information system be programmed to allow easy access to aggregate statistics on information transmitted to and from Canadian and foreign government agencies.

Further, a specific policy and auditing procedure should be developed for the release of any information on a Canadian resident.

Five Organizations

We reviewed operational files on five organizations representing different categories of counter-subversion targets, to determine whether investigation of these groups was warranted under sections 2 and 12 of the *CSIS Act*.

We compared the files with the relevant SERs and warrant affidavits, and we discussed our impressions with CSIS experts.

In making our own assessment of the Service's investigative effort against each of these targets, we considered the requirements of the *Act*, the magnitude and imminence of the threat as we saw it, and the extent of the resources CSIS was devoting to it.

We concluded that the Counter-Subversion Branch is primarily concerned with two things:

- The potential ability of foreign powers to manipulate Canadian policy through social institutions or legitimate protest groups.
- The possibility that certain groups might undermine Canadian institutions and bring about the violent overthrow of the state.

In both cases, there appeared to be an underlying belief that the Canadian public was only too liable to be duped.

We think that the Counter-Subversion Branch over-estimates the influence and persuasive power of these groups. From our own reading of the media and our own personal knowledge of people in every walk of life, we know that Canadians are generally mature enough to resist the blandishments of the groups concerned.

Over-estimated. We also believe that CSIS over-estimates the likelihood of violence by some groups.

One targeted group, for example, publishes a magazine that deals with a wide range of topics—the arts as well as social policy and other issues—from the perspective of the far left.

It is true that some members have advocated violent action by this group, but they were brushed aside by the others.

A good case could be made that the partisans of violence in this group rate investigation as individuals.

But we remain to be convinced that the group itself should be targeted for investigation. It opens the door to unnecessary intrusion on the freedoms and privacy of the most innocuous as well as of the most obnoxious members. It also carries the risk of harm to freedom of speech, one of our fundamental social values.

Summing up, it is possible that any targeted group could undertake terrorist acts at some point, but most are not, on the available evidence, likely to do so in the foreseeable future.

Two Paths

There are two paths running through the grey zone in which the Counter-Subversion Branch operates, corresponding to its two major concerns—undue foreign influence and the risk of violence.

As it happens, these are the concerns of two sister branches, Counter-Intelligence and Counter-Terrorism respectively.

We recommend that these two paths be followed to their conclusion. The counter-subversion role should be split between the other two branches; Counter-Intelligence would deal with undue foreign influence, Counter-Terrorism with the risk of violence.

Priorities could be set more rationally, and some of the targeted groups we have cited here might appear more clearly in their real light.

And good intelligence officers who may now feel isolated and ill-appreciated in the counter-subversion role would find themselves in more active environments where their talents would get full rein.

7. CSIS Itself

To end our review of oversight findings, we return to one of the questions we posed in Chapter 2: Is CSIS efficient—in terms of both management goals like financial integrity and policy goals like civilianization and official bilingualism? As the subject of a special inquiry, official bilingualism will be dealt with in the next chapter. This chapter focusses on other internal matters.

Resources and Administration

The obligation to spend public money wisely must always be a high priority, and it is doubly strong in times of restraint like these. All arms of government, including CSIS, are squeezed for funds.

But CSIS also has special problems all its own. It still faces one-time costs associated with "transition" as it creates facilities and services that were once the responsibility of the RCMP. These start-up cost have sometimes proved higher than expected.

The Service has also been asked to undertake new tasks without giving up old ones and, in some cases, without getting extra money or staff. In this connection, we welcomed the Government's decision to allocate a significant amount in 1986-87 for enhancement of the counter-terrorism program. We hope care will continue to be taken that CSIS is not forced to spread itself too thin.

Accommodations. Restraint has obstructed CSIS's program for providing all its staff with offices separate from the RCMP's. One effect, ironically, is to increase the ultimate costs, at least in current dollars, because of persistent—if relatively mild—inflation. Where CSIS has been unable to move out of RCMP accommodations on schedule, this may be an element in chilly mutual relations.

Following a report by the Auditor General on delays and cost overruns in renovating premises in Montreal, CSIS is developing a written accommodations policy and guidelines of its own to replace the RCMP policy and guidelines it had been using. It hardly needs to be said that we welcome this.

PEMS. In last year's annual report, we complained of weaknesses in the Service's PEMS (Policy and Expenditure Management System) documents.

CSIS has taken some positive steps since then. In last autumn's MYOP (Multi-Year Operational Plan), it used sub-elements that conform more closely to operational outputs (although some of them cannot be linked with distinct organizational entities, making it difficult to know who the responsible manager is). It is also attempting to show the marginal impact of security expenditures when it asks for funds.

On the other hand, we find that, though CSIS is fully meeting Treasury Board requirements, more recent MYOPs convey less information than earlier ones did.

For our own analysis, we wanted to know more, and CSIS has provided further information that has allowed us to examine spending as thoroughly as we did in previous years. We will make it a practice to ask for this information in future.

Civilianization

A major criticism of the RCMP Security Service was that it brought a police approach to security intelligence work.

The differences are important. As one study has noted, security work "offers few of the social and legal certainties" that the police can find in "the comparatively unambiguous objectives of prevention and apprehension".* We have aleady noted, for example, our own suspicions about the effect of the case-by-case police approach on the CSIS research effort (page 13).

The object of security intelligence work is not primarily to put miscreants behind bars. The core mandate is set out in the *CSIS Act* itself, which says (section 12) that the Service:

> shall collect ... and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

The McDonald Commission, like the Mackenzie Commission a decade or so before, recommended the creation of a civilian security intelligence agency, separate from the RCMP. "Civilianization" became one of the policy objectives underlying the *CSIS Act* adopted by Parliament in 1984.

Dedicated Service. For many reasons, CSIS will continue for many years to show its police origins. Most significantly, the RCMP Security Service had the only large pool of trained personnel it could draw on.

No exception can be taken to the fact that many CSIS intelligence officers (IOs) come from the Security Service; civilianization is something to work for today and tomorrow, not a reflection on invaluable work being done by dedicated men and women who got their start in the Security Service. In addition, it made sense for CSIS to rely on some RCMP accommodations and services. It would be unrealistic to expect anything different.

Nonetheless, we see a real need to keep prodding CSIS along the civilianization path. Table 2, opposite, shows the distance to be travelled.

CSIS seems to see the figures as an effective response to those who say it is just the RCMP without the Musical Ride; fewer than half its employees were once uniformed members of the RCMP, it points out.

We look at it another way: More than 80 per cent of the people at CSIS brought the memories and habits of work of the RCMP with them. While we have not yet obtained

* Richard French and André Béliveau, *The RCMP and the Management of National Security* (Montreal, Institute for Research on Public Policy, 1979), page 4

exact figures from CSIS, there is not the slightest doubt that the proportion is even higher in the key IO category and in middle management.

And this is after the "bridgeback" process was completed. In the two years ending July 16, 1986, former members of the RCMP had a right to return to the Force, and 75 did so—a relatively low proportion of those with bridgeback rights.

Table 2. Composition of All CSIS Staff

Former uniformed members of the RCMP	46 %
Former civilian members of the RCMP	15 %
Former public servants employed by the RCMP	21 %
Not formerly employed by the RCMP	17 %

(Source: as reported on December 3, 1986, by CSIS)

Who is Recruited

Recruitment from outside at all levels is the way to turn this situation around. We are seriously concerned by the reliance that CSIS has shown so far in its recruitment on "direct entries", as shown by Table 3.

Table 3. Sources of New IOs, January, 1985, to December, 1986

Public recruitment	51 %
Direct entry (mainly from police forces)	34 %
Conversions from within CSIS	15 %

(Source: compiled from CSIS figures)

Very nearly half the new IOs hired in 1985 and 1986 had police backgrounds. Direct entries are people with experience in police forces, the military and elsewhere, who are given IO status without going through basic training at the Service's own Sir William Stephenson Academy. The conversions are former surveillants who began their careers as RCMP "special constables".

The "not formerly employed by the RCMP" category in Table 2 includes some ex-police-officers from other forces, as can be seen, along with some other pertinent detail, in Table 4.

Apart from the fact that, as a good employer, CSIS should continue to make room in the IO category for surveillants and other employees with the requisite qualities, we think that the emphasis in recruitment should be on factors other than police experience.

Collecting information is only part of the job. The kind of information CSIS deals with is only as good as the analysis that's done on it and the advice that the government gets as a result. The emphasis belongs on solid training in scholarly research and the social sciences.

Table 4. IO Recruits Exempt from Training at the Sir William Stephenson Academy, January, 1985, to December, 1986

Source	Sex		Mother Tongue		Entry Level	
	M	F	Fr	Eng	IO-2	IO-3
RCMP	33	6	6	33		39
DND	2			2		2
PCO	1			1		1
CEIC		1		1		1
Other Police	5		1	4	1	4
Total	41	7	7	41	1	47

(Source: CSIS)

We also found that the appointment of direct entries at the "journeyman" IO-3 level is a source of resentment to graduates of the Academy, who start work at the lower IO-1 level (see page 45).

Time Out at the Academy

For a few short weeks, we felt reassured by the Service's written statements, in response to one of our formal queries, that it did not expect further direct entries at the IO-2 and IO-3 levels and that all new IOs—except some who are already on the payroll in other jobs—would go through the Academy.

But we were subsequently stunned to learn that CSIS had hired 16 former police officers in the last quarter of 1986 and left no positions open for new recruits from the universities or civilian employment.

As a result, the Academy has been closed down for a year, and further civilianization of the Service has stalled.

We understand that plans are being formulated to re-open the Academy in 1988. We strongly recommend that greater attention be given to civilianization and that, to that end, no direct entries be taken from police forces so a new class of civilian recruits can be made up as soon as possible.

Bilingualism and Equitable Participation

The 1987-88 class was to be the one in which, for the first time—CSIS management had solemnly decided some months ago—every member would be bilingual, as we have recommended.

It also offered the Service an opportunity to act on our repeated recommendations that it take steps to increase the representation of women and Francophones to levels closer to their representation in the labour pool.

Table 5 clearly shows why these recommendations need to be repeated and why the loss of the 1987-88 class will be so deeply felt.

Table 5. Selected Characteristics of CSIS Recruits in the First Three Classes at the Sir William Stephenson Academy (Percentages)

	January 1986	June 1986	February 1987
Bilingual (English-French)*	9	10	10
Women	25	20	10
First Official Language French	3	10	10

(Source: CSIS)

* CSIS reported that a further third of the first class, the entire remainder of the second class, and nearly a third of the latest class were composed of Anglophones with "some French".

The First Class

In our last annual report, we discussed our report entitled *Eighteen Months After: The Canadian Security Intelligence Service Recruitment, Training and Development Programs*. In the course of the research, we interviewed the first civilian recruits, who were then training at the Academy. We found that they generally had positive impressions of the training program.

Following up in 1986-87, we arranged new interviews with nearly half of the graduates of the first class. Except as noted below, morale remained high.

Overall, members of the first class enjoyed their work, found it challenging, and said they were pleased with their duties and ongoing development. On a scale of five, they gave an average rating of four to their feelings about CSIS. Most indicated that they expected to make a career within CSIS and rated their career opportunities as four on a scale of five.

Direct Entry. The one sour note, expressed by almost all those we interviewed, was that preferential treatment had been given to direct entries—that is, intelligence officers who have been recruited directly into CSIS because they have previous police experience.

The direct entry recruits are not required to take the introductory course at the Academy and they are generally hired at the IO-3 level (see Table 4 above), while civilian recruits are hired at the lower IO-1 level.

This represents a pay difference of about $10,000 a year, although the duties of an IO-3 and an IO-1 are broadly the same. The difference in level is based on the supposition that IO-3s are seasoned veterans who can be relied on to work more on their own and even to help IO-1s along.

This is frustrating to the IO-1s—so much so that we had some concern that valuable people might resign because they felt their career aspirations were blighted in this way from the start.

At another level, the advantage given to direct entries seems to perpetuate the domination of the Service by people who developed their corporate culture in police organizations.

These are both reasons to welcome new arrangements that will let superior IO-1s (usually civilian graduates of the Academy) reach the first level of management (IO-4) in as little as seven years—not the 11 years originally projected. But this is still much longer than the two years in which an IO-3 (ex-police direct entries) can hope to become an IO-4.

Training. Looking back from the vantage point of day-to-day work, the first class had varying comments on the training they got at the Academy. Overall, the basic suggestion was that training should concentrate more on everyday needs like source-handling, interviewing and report-writing.

Building Morale

We see value in a public relations campaign designed to foster an appreciation among Canadians of CSIS and its role. We think this could have a significant effect on morale, giving CSIS employees a positive corporate image to back up their own sense of personal contribution to the security of Canada.

A strong and positive image for CSIS could also overcome any gap between the corporate culture of ex-police-officers and that of employees who got their first taste of security intelligence work in the more civilian atmosphere of CSIS itself.

Polygraph Examinations

Another issue related to recruitment is the use of polygraph examinations. Despite one scrap of good news, we are disappointed with inaction at both CSIS and the Ministry of the Solicitor General on this issue.

In our last annual report, we set out in detail our grave doubts about the Service's use of the polygraph (popularly, though incorrectly, known as the "lie detector") in screening potential employees and in testing the loyalty of serving employees.

Testifying before the Standing Committee of the House of Commons on Justice and Solicitor General,* the Director said he was not satisfied that the opinion expressed by us and others was "sufficiently strong at this stage to warrant not proceeding with that particular investigative tool". He noted in particular that the polygraph examination is only one of 21 steps in the recruitment process and that any concerns raised by this test are pursued by investigation afterwards.

"I think were it so that the polygraph was used as the single tool for determining whether someone is being reticent or untruthful in terms of the answers provided, it would be quite wrong, and if that were the case we would not be using it", he told the Committee.

False Appearance. We think we met that argument last year when we said we could not believe that CSIS policy against making polygraph examinations the sole determinant of security clearances and employment could be made to stick. Because of their false appearance of scientific rigour, the results of polygraph examinations would more often than not be accepted at face value. There would be a strong temptation to discount a contrary result from investigation, because it was subject to "human fallibility".

Highlighting other arguments we made last year:

- There are no generally accepted scientific studies that establish the validity of polygraph examinations in mass employment and security screening (although we recognize that there may be a place for the polygraph as one of many tools in a criminal investigation).
- Even the defenders of polygraph examinations admit that the results are sometimes wrong—10 per cent of the time or more. Anyone who made spelling mistakes at that rate would be unemployable in a job that called for much writing, yet polygraph readings with less than 90 per cent reliability are wrapped in the cloak of "science" and can cost Canadians their careers and savage their reputations. Indeed, because of errors, polygraph examinations cannot even be defended as an airtight bulwark against penetration of the Service by disloyal and dishonest people.
- While polygraph examinations for serving members of CSIS were not mandatory, we did not believe they could be truly voluntary, as the Service claimed. Anyone who showed reluctance to be examined would inevitably be suspected of having something to hide, so the pressure to take a polygraph examination would be irresistable for all but the hardiest souls.
- Finally, we were concerned that as polygraph examinations became routine within CSIS, their use would spread throughout the government, bringing in their wake fear and mistrust—shabby values to encourage in a country like ours.

The good news since then is that CSIS has suspended its "voluntary" testing of employees already on the job. This disposes of one of the objections we made in our last annual report.

---

* House of Commons, *Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General*, December 11, 1986

But the rest of our doubts remain unanswered by either CSIS or the Ministry of the Solicitor General.

A Disguise. New recruits were still put through polygraph examinations, covering both lifestyle and loyalty, as a condition of employment. CSIS tried to dress its program up in a lab coat by calling it a pilot project, but this is merely a disguise.

The term "pilot project" suggests a trial run, carefully planned and equally carefully evaluated. This program has neither terms of reference nor evaluation methodology developed in advance of testing. In short, there is no "pilot project"—just the same old polygraph examinations continuing as usual under a new label.

Meanwhile, the issue has not been actively pursued by the Ministry of the Solicitor General.

Ministry staff told us they were awaiting the results of two studies taking place in other countries. Interested in these studies ourselves, we made inquiries and found that one had been cancelled and the second had been completed without yielding any useful results. We brought the Ministry up to date on these developments.

The Ministry, following the advice of an interdepartmental committee, contented itself with getting a legal opinion, which held that polygraph examinations could be considered a legal condition of employment.

Essential Flaw. This did little to resolve the issue of the essential flaw of polygraph examinations—their lack of reliability and the injustices that can flow from errors in reading their results.

We have heard reports that CSIS may be under some pressure from friendly security and intelligence agencies abroad to use polygraph examinations in security screening. We believe that these pressures should be resisted in the absence of conclusive evidence that polygraph examinations are more reliable than generally believed.

Indeed, we believe that well-designed, rigorous employment and security screening investigations would make the use of the polygraph superfluous in any case.

And we once again urge, as we did in our last annual report, that the use of polygraph examinations for employment and security screening be stopped and that a thorough and objective study be carried out so the Solicitor General and the Government can decide for themselves whether such methods are compatible with the values of our free and democratic society.

8. Closing the Gaps

Like civilianization, discussed in the last chapter, official bilingualism is a major policy goal for all federal agencies—and especially for CSIS, which has a lot of ground to make up.

At the request of the Solicitor General, we conducted an extensive inquiry in 1986-87 into official bilingualism and staff relations in CSIS, focussing on the Quebec Region, the Ottawa Region and Headquarters, where tensions seemed to be highest.

Culture and Communications. Our report, submitted to the Solicitor General in March, 1987, highlights gaps in culture and communications and makes a total of 48 detailed recommendations for bridging them. CSIS management has undertaken to make a conscious and sustained effort to close these gaps. To provide an overall framework, we recommended that:

- A Deputy Director, Special Projects, be appointed for a two-year period to oversee implementation of a special official languages plan and of our recommendations for better staff relations.
- A consultative committee of experts—from Treasury Board, the Department of the Secretary of State and the private sector, perhaps—be created to assist in implementing the official languages plan.

We prepared an abridgement of the report to permit broad distribution. We are now informed that it will be made public.* As we say in our preface to the abridgement: "We hope this signals the Service's determination to lay the ghosts of past problems and get on with the tasks of giving both official languages their due and opening up channels of communications in staff relations".

We will continue to follow the official languages and staff relations issues closely.

In this chapter, we review some of our most important findings and list other major recommendations.

Official Languages

We found in our special study that, despite good intentions at the top, there had not been enough real commitment among some key players to the government's official languages policies and not enough understanding of the Francophone culture that shapes the thinking of one in four Canadians.

CSIS was taking steps to improve the situation. During our inquiry it:

- Lifted a moratorium on language training and on the usual obligation that a unilingual government employee faces to learn the second language within two years of appointment to a bilingual position.
- Hired a Chief, Official Languages, who immediately went to work drafting key policies.

---

* *Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service* (Ottawa, 1987)

We welcome these initiatives. But our optimism is clouded by lapses that continue to take place.

Indeed, it has since become difficult to resist a tinge of cynicism as a result of a mismatched pair of decisions about the Sir William Stephenson Academy, where training is provided to new intelligence officers.

During our inquiry, management decided that henceforth all recruits admitted to the Academy would have to be bilingual and courses would be given in both official languages. Later (see page 44 of this annual report), it undermined its credibility by suspending classes at the Academy for a year.

One lapse during the inquiry itself was the publication of a Directive Writers' Guide in English only—despite the basic principle that employees whose working language is French are entitled to the same assistance in carrying out their duties as those whose working language is English.

Culture gap. This is a small but telling example of what we meant by the "culture gap"—the expectation some Anglophones seem to have that Francophone needs can be dealt with as an afterthought. We want to make it clear that this approach was not universal, but we caught whiffs of it far too often for our liking.

Complaints about messages to the Quebec Region in English only or in English first with a French translation later, sometimes much later, were among the issues that led to our inquiry. Yet such messages remained a problem at least as late as October, 1986—seven months after our inquiry began.

English-only messages from Headquarters clearly contravened government-wide official languages policy. Officially designated a bilingual office with French as its primary working language, the Quebec Region is entitled to get communications from Headquarters either in English and French simultaneously or in French alone.

Spirit of Bilingualism. Frequent English-only messages from one Ottawa Region unit to the Quebec Region were, strictly speaking, admissible under official languages policies. Designated a bilingual office itself, Ottawa Region is entitled to communicate with all other CSIS offices in either or both official languages.

However, we consider that this particular unit is in a special position because it provides a national service to all branches of CSIS, coast to coast, and the spirit of official bilingualism calls for more than the strict minimum.

We were often confronted with the "urgency" argument—that translation into French would impose unacceptable delays. We found that there was usually less to this argument than met the eye. In many cases, for example, material in a foreign language was translated into English; why could it not be translated into French at the same time?

Other Issues. Among other issues were a very modest level of bilingualism required in some Headquarters positions, the advertisement of positions before the language requirements had been approved by the Chief, Official Languages, and failure to consider equita-

ble representation in the selection of the first class at the Sir William Stephenson Academy with the result that only one recruit was Francophone ("We goofed", one highly-placed source admitted to us).

Anglophone Concerns. At the same time, we noted concerns among unilingual Anglophone employees that strict adherence to the government's language policies could stall their careers.

We believe that stepped-up language training is the way to make it clear that there is equal opportunity in CSIS for all qualified people, regardless—to borrow the wording of the *Canadian Charter of Rights and Freedoms*—of race or national or ethnic origin.

Recommendations. Among our major recommendations for dealing with official languages issues were that:

- A special, two-year official languages plan be implemented to make up for lost time.
- CSIS give priority to expanding its facilities for translation into French so that operational efficiency ("urgency") could no longer be offered as an excuse for English unilingualism in written communications.
- As a matter of policy, the Ottawa Region unit mentioned above communicate in French with French-language offices and bilingual offices where French is officially designated as the primary working language.
- A French-language equivalent to the Directive Writers' Guide and any other guides or manuals now available in English only be published in 1987.
- Steps be taken to ensure that management positions are designated bilingual on the same basis as this is done throughout the government and that no job competition be held until the Chief, Official Languages has established official languages requirements for the position concerned.
- Language training be scheduled by the end of the Special Plan for all unilingual employees in bilingual positions and that CSIS officially decide by July 31, 1987, how it will deal with unilingual employees in bilingual positions who (a) are not eligible for second-language training, (b) refuse or fail to enrol in such training, (c) fail such training or (d) lose their ability to work in the second language.
- Continued emphasis be placed on bilingualism as a recruitment criterion and that CSIS structure its hiring and staffing procedures to ensure adequate Francophone recruitment.
- The bilingualism bonus be paid in accordance with Treasury Board rules.

Haig-Brown. Because there have been reports in the media on the so-called Haig-Brown Report, it may be worth briefly saying what we found in the course of our inquiry.

This report, a collection of memoranda by two Army officers seconded to the RCMP during the Second World War to advise on the organization of personnel selection, perpetuated unacceptable stereotypes about certain ethnic groups.

We were not entirely convinced by protests that the Haig-Brown Report was irrelevant in its day, but, in the final analysis, we agreed that its present interest is historical; there is no evidence that it ever guided personnel selection in CSIS.

OCOL. We should also say for the record that we conducted our inquiry in cooperation with the Office of the Commissioner of Official Languages (OCOL), which was simultaneously engaged in its own audit of official languages practices at CSIS. OCOL was issuing its own report.

Staff Relations

We found that real problems in staff relations had been amplified by a communications gap in which management and some employees came to suspect the worst of each other.

The problems and the communications gap could both be traced in part to transition, as CSIS took shape out of the former RCMP Security Service. CSIS managers themselves acknowledge that in the hectic early days, many decisions were founded more on intuition and experience than on planning or policy. It is hardly surprising that such decisions sometimes seemed arbitrary and lent credibility to whispering about discrimination and favouritism.

Another factor was nostalgia for the RCMP. Managers who learned their craft in the hierarchical RCMP tended to expect swift and silent obedience, not questions about their decisions.

Finally, there was the value attached to the need-to-know principle in any security and intelligence agency. This principle is, of course, essential in security matters. But it should not spill over into routine administrative matters. CSIS had not made known, for example, its policy governing transfers.

Personnel Manual. As in official languages, CSIS was taking steps to deal with its staff relations problems. We were especially reassured to find that it was preparing a formal Personnel Administration Manual. By clarifying the rules, this Manual can prevent much misunderstanding and suspicion.

CSIS is also proposing that the Public Service Staff Relations Board (PSSRB) be empowered to adjudicate grievances by non-unionized employees like intelligence officers, surveillants and analysts. At present the Director makes the final decision on these grievances, which places him in the awkward position of being both judge and party.

Our only concern is to ensure that the amendment sought to the *Public Service Staff Relations Act* actually does give the PSSRB an adequate mandate to deal with CSIS grievances.

Conversion. One of the major controversies that led to our inquiry had to do with "conversion", when surveillants (former "special constables" in the RCMP, the people who tail targets) were given an opportunity to compete for positions as intelligence officers (IOs).

This was an opportunity of great significance to the surveillants. Their jobs lead nowhere; the reward for diligent and skillful surveillance is the chance to do more surveillance. An IO, on the other hand, is on the first rung of the career ladder that leads to the director's office.

Communications problems, unfortunately, turned conversion into a battlefield. In the first place, surveillants interviewed in the course of our inquiry believed that the distinction between them and IOs would be completely erased; all would be on the same career path. At least some surveillants in Montreal believed that they were being offered absolute priority to try for IO positions before any outsiders were considered.

Both these hopes were dashed. CSIS management interprets the promises it made much more narrowly. It believes that it kept its promise by letting the surveillants apply for jobs as IOs without holding university degrees (which few surveillants have) or going through basic training at the Sir William Stephenson Academy.

Mobility Agreement. The Montreal surveillants also believed that a mobility agreement presented to them as a condition of conversion was an attempt to frighten them off. This agreement raised the possibility of transfer, and the surveillants lived up to the conventional wisdom that Francophone Montrealers in all fields prefer to make their careers in Montreal.

In a serious departure from good official languages practice, CSIS first offered psychological testing in English only, then made those who insisted on French tests wait for six months. Only the "culture gap" we referred to under the official languages heading above can explain this kind of unequal treatment of Francophone and Anglophone candidates for conversion and failure to anticipate the reaction.

Then came the announcement of a second conversion competition before the first one was completed in Montreal. The Montreal surveillants were apparently not told that the first competition was over in the rest of the country, and they were quick to conclude—understandably if, as best we could determine, wrongly—that this was a dirty trick of some kind.

Other Problems. Our findings on the grievance procedure are obvious from what we have already said and from the recommendations described below.

We also found that the prospect of ill-explained lateral transfers was a serious source of insecurity among employees, that there was a widespread belief that competitions for promotions concealed rather than prevented favouritism, and that CSIS employees (who are not, legally speaking, public servants) feel trapped because they cannot enter internal competitions for Public Service jobs.

Recommendations. Among our major recommendations for dealing with staff relations issues were that:

- The *Public Service Staff Relations Act* be amended in such a way that grievances by non-unionized CSIS employees can be adjudicated by a member of the Public Service Staff Relations Board with suitable security clearance.

- Since non-unionized employees do not have a collective agreement, they be allowed to grieve on the basis of the Personnel Administration Manual.
- The Director's reply to a grievance always include reasons for the decision.
- Arrangements be made for paycheque deductions to provide the Association of CSIS Employees with funds to pay the costs of adjudication if the Association decided to accept a role in such proceedings. The amount of the checkoff would be determined by a majority vote of Association members.
- CSIS issue a policy statement describing career paths open to its employees, especially those outside the IO category, and setting out the rules for conversion from one path to another.
- CSIS issue a policy statement specifying the conditions under which lateral transfers will be made.
- In staffing, selection boards be composed of the supervisor to whom the position reports, a supervisor of equal rank from another branch of the Service and an officer, with appropriate security clearance, of the Public Service Commission.
- CSIS explore avenues for permitting its employees to compete for Public Service jobs.

9. Complaints

Citizenship and immigration cases gave us most of our work on complaints in 1986-87.

This was not merely a matter of numbers. Compared with security clearance cases, those dealing with citizenship and immigration are complex and difficult, usually involving large numbers of reports and documents accumulated over many years. And the stakes are high. An adverse report by us could well result in the Governor in Council's deciding to deny citizenship or direct the commencement of deportation proceedings.

Meanwhile, the number of new complaints about security clearances plunged.

Kudos for Defence

New screening procedures at the Department of National Defence (DND) appear to go a long way to explaining the drop in security clearance complaints.

In our last annual report, we objected in strong terms to the way DND had carried out clearance investigations.

We are pleased this year to say publicly what we have already said privately—that DND showed some real sensitivity to individual dignity by radically revising its security clearance procedures.

Of the 44 people whose cases we asked DND to reconsider in 1986, fully 39 were granted clearances. The other five withdrew their complaints on promises that their cases would be re-examined at a later date.

New complaints against DND in 1986-87 totalled zero. We hope that this Department maintains the high standard it has set for itself. As insurance, we have asked it to tell us every year how many security clearances it has denied. If the number is high, yet complaints are low, we will ask why.

Security Clearances

The number of new complaints arising out of security clearances denied by other departments also shrank; there was only one in 1986-87, compared with 14 the year before.

We like to think that this reflects greater care being taken as the people responsible for security—in departments and agencies as well as in CSIS—learn about the complaints process and the criteria that are taking shape as we deal with specific cases.

A new security classification and screening system was introduced by the Government in 1986. It does not come directly under our oversight mandate. But it is an important element in complaints that we hear as well as in CSIS's workload, so we say something about it later in this chapter.

Mandates. Under the *CSIS Act* (section 42), a complaint can be made to us by:

- A person refused federal employment solely because a security clearance has been denied.

- A federal employee who is dismissed, demoted or transferred or denied a promotion or transfer for the same reason.
- Anyone refused a contract to supply goods and services to the government for the same reason.

The Department of National Defence carries out its own security screening.* In other departments and agencies, decisions to grant or withhold clearances are made by the deputy head after a security assessment is submitted by CSIS.

Anyone denied a clearance must be notified and told that a formal complaint can be lodged with us. After investigation and *in camera* hearings by one or more members of our Committee, we report our findings and any recommendations to the Solicitor General, the Director of CSIS, the deputy head concerned and the complainant.

Investigations and Recommendations. This year, hearings have been completed and recommendations made in two cases. In one we recommended that clearance be granted, and this was done. In the other we supported CSIS's recommendation against clearance. Summary case histories can be found in Appendix B. One complaint of this kind was still under investigation at year-end.

Complaints against CSIS

Mandate. The *CSIS Act* directs us to investigate complaints about "any act or thing done by the Service" (section 41).

There are two principal limitations. A complaint must first be made to the Director of CSIS. We can then accept the complaint if the Director has not responded within a period that we consider reasonable or if the complainant is not satisfied with the Director's response.

Second, we may not investigate a complaint that can be channeled through another grievance procedure under the *CSIS Act* or the *Public Service Staff Relations Act*.

Complaints by Employees. Both we and the Commissioner of Official Languages received 1,776 complaints in 1986-87 about the Service's official languages practices, all from CSIS employees. This is about three times the number of language complaints in the previous year.

We held these complaints in abeyance while the Office of the Commissioner made a detailed audit of official bilingualism in the Service and while we conducted the inquiry reviewed in Chapter 8.

Complaints from the Public. We had 13 complaints from members of the public, compared with four in the previous year. Twelve, mostly from disappointed candidates for

* So does the RCMP.

employment by CSIS, were outside our jurisdiction and one was under investigation at year-end.

Immigration and Citizenship

We had 13 citizenship cases and one immigration case on hand as 1986-87 began. Five more immigration cases came to us during the year, but there were no new citizenship cases.*

Mandates. Under the *Citizenship Act*, the Secretary of State reports to us when he is of the opinion that citizenship should be denied because there are reasonable grounds to believe that the applicant is either a threat to the security of Canada or is involved in organized crime.

Similarly under the *Immigration Act, 1976*, a report is made to us when the Minister of Employment and Immigration and the Solicitor General believe that the applicant for admission to Canada will engage in activities inimical to Canada's interests in various specified ways.

In both cases, the subject of the report must be notified. We investigate as we would in the case of a complaint by an individual and make recommendations to the Governor in Council.

Investigations and Recommendations. One immigration case was disposed of. We agreed that admission to Canada should be denied. Investigation was continuing on four immigration cases and a fifth was being reopened by consent of all parties.

Six citizenship cases were closed. In two, we recommended that citizenship be granted. One citizenship case ended when the applicant died. In addition, CSIS withdrew its objections in three citizenship cases during investigation. Summary case histories of citizenship and immigration cases can also be found in Appendix B.

One report on a citizenship case was being prepared at year-end, and investigation was continuing in six cases.

The first case involving the criminality provisions of the *Immigration Act, 1976*, came to us at the close of the year. There was reason to expect more early in 1987-88.

Quality of Investigations

We have already dealt with the striking improvement in the quality of investigations by the Department of National Defence.

---

* Readers who enjoy statistical analysis may want to know that: (a) one of the immigration cases and one of the citizenship cases involve the same person, and (b) one of the new immigration cases is identical with one of the immigration cases carried over from the previous year; it is being re-opened with the consent of all parties.

CSIS Security Assessments. Over the last three years, we have seen many security screening reports prepared by CSIS for other departments and agencies, and, for the most part, they were well done.

However, in the cases we saw this year, some conclusions were inferred from insufficient evidence and what could have been perfectly innocent activities were sometimes viewed in the worst possible light without adequate reason. Case reports highlighted these weaknesses.

Immigration and Citizenship. We were especially disappointed in the quality of CSIS reports and of the evidence it presented to us in citizenship and immigration cases.

For example, the Service sometimes took weeks to respond to straightforward questions that we posed during the preliminary investigation, and it sometimes came to hearings with evidence that had not been seen by the minister or ministers to whom the initial recommendation had been made.

Neither the delays nor the after-the-fact accumulation of evidence speaks well of the care taken with recommendations on which the rest of a person's life may depend.

Special Report. We have made a special report to the Solicitor General, under section 54 of the *CSIS Act*, to share with him our concerns about both security assessments and the handling of citizenship and immigration cases by CSIS.

A special report was necessary because CSIS does not accept our concerns. In fact, CSIS seems to blame the process required under the *Act*—or our interpretation of the process.

To bring about better controls, we recommended that:

- The Director (or, in his absence, a deputy director) of CSIS personally have sole authority to recommend that, for security reasons, citizenship be denied, a potential immigrant or visitor be refused entry or a permanent resident be deported.
- These recommendations be made to the Solicitor General who, if he agreed, would then, in citizenship matters, authorize the report being forwarded to the Secretary of State or, in immigration cases, would forward the report himself, with his own comments, to the Minister of Employment and Immigration.
- Similarly, the Commissioner of the RCMP (or, in his absence, the Deputy Commissioner) personally be the only one with authority to make recommendations to the Solicitor General regarding deportation under the criminality provisions of the *Immigration Act, 1976*.
- Only the Director of CSIS (or, in his absence, a deputy director) have the authority to recommend that a security clearance be denied to a Canadian seeking federal government employment.

We look forward to discussing this issue in detail with CSIS, and we hope next year to report that more effective procedures have been developed for maintaining the delicate balance between protection of the security of Canada and protection of individual rights.

Immigration Act Study

In a report on June 17, 1986, the Standing Committee of the House of Commons on Labour, Employment and Immigration made two recommendations regarding security screening, as follows:

> 32. The Solicitor General should ask the Security Intelligence Review Committee to investigate and report on whether Canada's *Immigration Act* is adequately protecting Canada and any recommended legislative changes should be introduced to Parliament as soon as possible.
>
> 34. The Solicitor General should ask the Security Intelligence Review Committee to review the criminality provisions of the *Immigration Act*.

On September 26, 1986, the Solicitor General officially asked us to investigate and report on the effectiveness of the relevant provisions of the *CSIS Act*. Under Section 40 of this *Act*, we have asked the Inspector General to undertake some fact-finding for us. Our work on this was continuing at year-end.

We have also been invited to take part in the Interdepartmental Working Group formed by the Minister of State (Immigration) to develop the Government's response to the Standing Committee's report. We are represented by the Executive Secretary.

In neither of these activities do we play an executive role. But our experience with immigration and the virtually identical citizenship cases has given us a particular perspective that we feel should be put at the Government's disposal as it considers amendments to the *Immigration Act, 1976*.

We regard it as preventive action. Better to offer our advice now in hopes of warding off problems than waiting for problems to emerge and then carping from the sidelines.

The New Security Policy

On June 18, 1986, the then Solicitor General introduced a new security policy and operational guidelines for classifying information and screening personnel.

The previous policy had its origins in a 1956 PCO document called Security of Information in the Public Service of Canada, supplemented by Cabinet Document (CD) 35, which dates from 1963. It is generally recognized that too much information was being classified and security clearances were being sought for too many people under these arrangements.

Costs are a factor in limiting the scope of security policy. The average cost of a Top Secret clearance has been reported as $1,425 and of Confidential and Secret clearances as $13.62—figures that we believe are, if anything, serious underestimates, as we explained in last year's annual report.

Speeding up the screening process for individuals by reducing the demand was another reason for reform. As matters stood, CSIS was snowed under by a growing backlog of clearance investigations in progress. This situation, too, we described in last year's annual report.

Demand. The new measures were to bring about a reduction in the demand for security clearances by requiring that requests be justifiable, equitable and effective. It established as objectives that:

- Only information whose protection from unauthorized disclosure is essential to the national interest be classified.
- Departments and agencies reduce the number of positions that require employees to be security cleared.
- The rights of individuals affected by the government's administrative security system be improved.
- The security of Canada be upgraded by more effective management of the resources dedicated to the security screening and information classification and protection programs.

Under the new policy, information is to be classified only if it falls into one of six categories—national defence, international affairs, national security (including hostile and subversive activities and threats to the security of Canada), Cabinet confidences, federal-provincial affairs, and selected economic interests of Canada.

Deputy heads are held accountable for security in their departments and agencies. Among other things, they identify employees who need security clearance and ensure that, as a condition of employment, these employees are screened.

Except, as explained above, in the case of DND and the RCMP, a "security assessment" is provided by CSIS. But the ultimate decision to grant or withhold clearance lies with the deputy head.

Rejection Criteria. Under the new policy, no one can be refused security clearance for disloyalty unless there are reasonable grounds to believe that he or she engages in or may engage in activities that fall within the definition of "threats to the security of Canada" in the *CSIS Act* (section 2).

Under CD 35, a person could be rejected for "unreliability", not merely for outright disloyalty. This remains true, but there must be reasonable grounds to believe that the individual may disclose (through careless talk, for example) or may be induced to disclose (under the threat of blackmail, for example), or may cause to be disclosed (through habitual carelessness, for example) classified information.

Treasury Board, which is responsible for the overall management of the new policies, is assisting each department with implementation of the program and monitoring compliance with the new policy.

On September 12, 1986, the Solicitor General issued a formal directive to CSIS governing the provision of security assessments.

Redress. Announcing the new security policy, the then Solicitor General reaffirmed that the Government was committed to a fair and equitable review procedure for those denied security clearances. He said:

> Members will know that the SIRC is made up of five Privy Councillors representing all three parties in the House. It has an independent mandate to review all complaints concerning security clearances requested by the government, with full authority to require the production of evidence and witnesses from the Service and the department that has denied the security clearance.
>
> The SIRC has demonstrated its value as a review mechanism by the careful, thorough and fair manner in which it has investigated and reported upon those cases which have so far come before it and the way in which it has brought the principles of natural justice into play in these cases.*

Impact on CSIS. We have not conducted a full review of the new security policy's impact on CSIS. However, we are mindful of three elements that will add to its workload, as follows:

- CSIS will establish and maintain a central index for all security clearances.
- For criminal records and credit checks, it will be the sole entry point for all agencies except DND and the RCMP on security screening.
- As a pilot project, personal interviews are to be conducted with persons requiring Secret clearance, whereas interviews were previously conducted only for cause. Personal interviews are now always required for Top Secret clearance.

No Let-Up. Six months after the announcement of the new policy, our research showed no let-up in requests for security assessments. As a matter of fact, while requests for field investigations—more or less synonymous with requests for Top Secret clearances—were down, total numbers increased after the new policy was in place. Table 6 sets out the figures for the last six months of 1985 and of 1986.

Table 6. Requests for Security Assessments

	security clearance requests	field investigation requests
second half, 1985	31,797	2,005
second half, 1986	35,061	1,425

(Source: CSIS)

* *House of Commons Debates*, June 18, 1986

These numbers include all three levels of clearance—Confidential, Secret and Top Secret.

The Solicitor General has taken a number of steps to deal with this situation.

At a mundane but practical level, he directed the Security Screening Branch at CSIS to get the temporary secretarial help it needs to clear the backlog of about a thousand cases that had been wrapped up by the investigators but remained piled up in the typing pool In basket.

He also directed the Service in December, 1986, to send outstanding requests back to the departments for reconsideration under the new policy.

Finally, he asked the Intelligence and Security Co-ordinator at the Privy Council Office to speak personally with deputy heads in departments that may be asking for Top Secret clearances that cannot be justified under the new policy.

10. Tidying Up

Our work in oversight and complaints is no mystery to readers of the foregoing chapters. But some of our activities do not fit under either of these rubrics. We describe them here.

Answering to Parliament

We appeared twice in 1986 before the Standing Committee of the House of Commons on Justice and Solicitor General—on June 3 to answer questions on our 1984-85 annual report and on November 20 to answer questions on our 1985-86 annual report. Issues raised with us on those occasions have been dealt with in this report.

As the year under review ended, we looked forward to an appearance before the Special Senate Committee on Terrorism and the Public Safety on April 3, 1987.

Outreach

As part of our accountability to Parliament, we see ourselves as accountable to Canadians at large.

Accepting a responsibility to foster public knowledge and awareness of security and intelligence matters, we are as forthright as security considerations let us be with the hundreds of individuals who ask us about security clearance procedures and about specific incidents or general issues.

Mass Media. We are as open as possible with the mass media. After our second Annual Report was tabled in Parliament in June, 1986, we held a news conference, and our Chairman, the Honourable Ronald G. Atkey, as well as other members and staff have been interviewed many times over the year. We believe that in a healthy democracy there can and should be a degree of informed public discussion on national security issues.

There are also occasions when it would be inappropriate for CSIS to make issues public but it is appropriate for us to do so. On such occasions we are able to put matters in perspective, to the benefit of all concerned.

Meetings and Conferences

Academic researchers and students also interview the Chairman and staff. We keep our lines open to academic and professional specialists in security intelligence, not only out of a duty to share our own insights widely but for what we can learn from them.

In the past year, the Chairman:

- Was a panelist at the National Forum on Access to Information and Privacy staged by the Department of Justice and Treasury Board March 7, 1986.
- Presented a paper entitled "The Security Intelligence Review Committee: Legislative Oversight and Government Policy in Canada Today" at a conference on Intelligence and Policy sponsored by the Defence Intelligence College in Washington, D.C., August 26-28, 1986.

- Spoke on "Accountability of the Security Intelligence Committee" at a seminar organized by Professors Clifford Shearing and Stuart Farson at the Centre of Criminology in the University of Toronto, February 24, 1987.
- Spoke to Osgoode Hall Law School students at York University enrolled in a course on security and intelligence, March 11, 1987, and participated in discussion afterwards. The session was organized by Professor Peter Hanks, a visiting professor from Australia.

Two members, the Honourable Jean Jacques Blais and the Honourable Frank McGee, attended the National Conference on Law in Relationship to Terrorism, sponsored by the American Bar Association in Washington, D.C., June 5-7, 1986.

Our Executive Secretary and a research officer participated in a conference on The Psychology of Terrorism in Washington, D.C., at the Woodrow Wilson Center, International Security Studies Program, March 16-17, 1987.

In addition to attending the August 26-28, 1986, conference on Intelligence and Policy sponsored by the Defence Intelligence College in Washington, D.C., with the Chairman, the Director of Research attended the second annual conference of the Canadian Association of Security and Intelligence Studies at the University of Manitoba in Winnipeg, June 7, 1986.

The Executive Assistant and the Senior Complaints Officer met twice with U.S. Defence Department officials to study personnel security policy and exchange ideas—first at the Pentagon on November 14, 1986, and then at the Personnel Security Research and Education Center in Monterey, California, on January 15 and 16, 1987. At the Research and Education Center, the Executive Assistant made a presentation on the development of the security screening process in the government of Canada.

A research officer attended a symposium on Present and Future Strategies for Employment Testing on June 21, 1986, at the annual conference of the Canadian Psychological Association.

Personnel

Our office remains as lean as it was at the end of last year; throughout 1986-87, we still had just 13 employees, despite a mushrooming workload.

They are headed by an executive secretary who directs all day-to-day operations. Other employees are a research director, two researchers and a research assistant, a senior complaints officer, an executive assistant who supports the research and complaints functions, an administrative officer who is also the registrar for our hearings and coordinator of our response to requests under the *Access to Information Act* and the *Privacy Act*, and five support staff. A complete list with telephone numbers can be found in Appendix C.

Financial Report

Our 1986-87 budget is set out in Table 7. We originally budgeted $344,000 for goods and services in 1986-87, but found that this amount had to be nearly doubled through supple-

mentary estimates to meet needs that could not be foreseen when the main estimates were drawn up in 1985—notably:

- Conducting, at the request of the Solicitor General, a special study of official languages and staff relations problems in CSIS (see Chapter 8, page 49 of this annual report).
- Meeting legal fees associated with the complaints process.

Table 7. SIRC Budget, 1986-87

Personnel		$545,000
Salaries and wages	$475,000	
Contributions to employee benefit plans	$70,000	
Goods and services		$677,000
Professional services	$519,000	
Other	$158,000	
Total operating expenditures		$1,222,000
Capital expenditures		9,000
TOTAL		$1,231,000

(Source: 1987-88 Estimates, Part III)

11. Looking Ahead

Among our priorities for 1987-88, we number CSIS's counter-terrorism program, its intelligence analysis and production process, and the protection of scientific and technical secrets.

Our work on the protection of scientific and technical secrets has already begun, and we might say a word about it here, to set the scene.

Science and Technology. Traditional military secrets are no longer the only targets of espionage. Scientific and technical knowledge must also be protected. Being a member of the Western scientific community as well as of Western military alliances, Canada has a duty to safeguard borrowed as well as home-grown science and technology.

We are looking into a number of issues that arise out of these considerations, including:

- CSIS's part in developing policies to protect scientific and technical assets—ours and our allies'.
- What intelligence CSIS provides to federal departments involved in export controls and other protections for secret scientific and technical knowledge.
- The priority CSIS gives to collecting intelligence on the theft of science and technology and what resources it devotes to this task.
- Whether the government's identification of potential targets is adequate.
- What provisions are made for security screening personnel in high-technology firms that have access to secret scientific and technical knowledge.

We have had briefings from CSIS on these matters and are pursuing our inquiry.

Five-Year Review

But our overriding preoccupation in the coming year will be to draw up a full list of issues that Parliament may want to address when it conducts the five-year review of the *CSIS Act* in 1989.

We intend to consult with interested individuals, with relevant interest groups and with experts in the universities, government and elsewhere. This will allow us both to test the conclusions we have drawn from our experience and to provide them with an early forum for insights we may profit from.

Scattered throughout this report are issues that have suggested themselves in our routine review activities—for example, the protection of solicitor-client privilege (page 19) and the adequacy of raw warrant statistics (page 11).

The Extent of Oversight

Another issue we can already see on the horizon is the oversight function itself. The *CSIS Act* broke new ground when it created this Committee to monitor the Service. But there

are other major players in the Canadian security and intelligence community and they are not in the purview of any independent oversight.

Canadian Security and Intelligence Directory. Indeed, one of the surprises we got when we took up our duties in 1984 was that we could not even find a comprehensive directory of federal government agencies engaged in security and intelligence work.

We felt it was important to know something about CSIS's sister agencies. For one thing, we would better understand CSIS's mandate if we knew the mandates of the others and CSIS's relationships with them. We were particularly interested in committees that disseminate security and intelligence information and that make decisions based on this information. Knowing the needs of such committees would improve our appreciation of CSIS's operational objectives and its relationships, real and potential.

Unable to find a complete directory, we decided to prepare one ourselves, and this task was completed in 1986-87.

We recognize, with regret, that we cannot make the directory public. Some of the material it contains—notably descriptions of the roles played by certain agencies—would be of far too much interest to the enemies of our country. We also promised to limit circulation in order to gain the cooperation of certain agencies that had no legal responsibility to provide us with information.

However, we have made copies available within the Canadian security and intelligence community itself and have been pleased with the very favourable reactions. Apparently we were not alone in feeling that it is useful to know just who does what.

Because of these reactions, we intend to revise and distribute the directory yearly, both to keep our own understanding up to date and to serve the security and intelligence community within Canada.

Cabinet Confidences. Another limit on our present powers is that we are not entitled to be told Cabinet confidences. We have not felt this as a severe limitation to date but, of course, we cannot really assess how much we are missing. We have been concerned that it could be a problem if a Cabinet spread the mantle of confidentiality too widely in future.

We note that the Standing Committee of the House of Commons on Justice and Solicitor General has recommended tightening the definition of Cabinet confidence for purposes of the *Access to Information Act* and the *Privacy Act*,* and we await the Government's response before taking a more precise position of our own.

---

* House of Commons, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, Report of the Standing Committee on Justice and Solicitor General on the review of the *Access to Information Act* and the *Privacy Act*, March, 1987

A Last Word

At the middle of our five-year mandate, we look back with some satisfaction on what we have been able to do—and forward with not a little apprehension to how much more we have to do.

Yet in reflecting on our work to date, we continue to value two important features of our mandate. The first is our appointment as part-timers, active on other matters in the community and in private life. This has permitted us to remain somewhat more objective and detached from the day-to-day intrigue of security intelligence matters specifically and government affairs generally. Hopefully it has sharpened our analysis and judgement.

Second, we have had the good fortune to attract competent and hard-working professionals as members of our permanent staff and panel of outside consultants and lawyers. All of these Canadians, after achieving the appropriate level of security clearance, have thrown themselves into the task at hand with dedication, energy, and a strong sense of commitment. Treasury Board has responded positively with a level of resources which is limited but nevertheless appropriate. The Committee and hence Canadians are well served by this group of "watchdog" professionals who work long and lonely hours mostly without public recognition—except that which it is our pleasure to provide in this report.

Appendix A

Ministerial Directives and Directions to CSIS, 1986-87

CSIS-RCMP Cooperation Regarding Counter-Terrorism

The Provision of Security Assessments

Notification of the Minister Concerning Certain Types of Operations

Investigative Activity

Use of Confidential Sources

Protection of Canadian Citizens

Protection of Foreign Citizens in Canada

Policy on Reporting Incidents to the Minister

Arrangements for RCMP Assistance

Appendix B

Summary Case Histories of Security Complaints Dealt With by the Security Intelligence Review Committee, 1986-87

Security Clearances

1. A person complained that a Top Secret clearance was denied on the basis of alleged dishonesty in (a) citing false past job titles on a personal history form, (b) misappropriating the employer's property in a past job and (c) having been involved in the sale of stolen goods.

At the hearing, CSIS cited reports from its sources in support of all three allegations. A CSIS investigator answered detailed questions about the reliability of these reports.

The complainant denied all allegations, noting that employer statements confirmed the accuracy of the job titles and arguing that personal animosities lay behind the other allegations. The complainant further argued that the allegation about the sale of stolen goods involved mistaken identity.

The Presiding Committee Member found that the job titles had not been misrepresented, but sustained the other allegations.

The Presiding Committee Member recommended that the denial of a Top Secret clearance be upheld.

2. An individual was denied the Top Secret clearance required for transfer to a special unit. Denial was based on alleged dishonesty, indiscretion, and financial indebtedness.

The allegation of dishonesty turned out to be based on a minor, isolated incident that did not justify continuing concern, and the indiscretion issue proved to be groundless.

But the heavy indebtedness was real, and CSIS held that the resulting financial pressure could tempt the complainant to offer favours to clients in return for cash. It could also tempt knowledgable clients to offer financial inducements.

However, CSIS acknowledged that there was nothing to indicate that the complainant could not overcome the indebtedness by honest means; indeed, it agreed that the complainant deserved credit for positive efforts to deal with the problem.

An official of the employing department testified that, after interviewing the complainant, he was satisfied with the explanation provided for the indebtedness.

Finding that the complainant had the indebtedness under control and that all other allegations were groundless or minor, the Presiding Committee Member recommended that Top Security clearance be granted.

Citizenship

3. Citizenship was denied to a landed immigrant, 14 years in Canada, when CSIS said there were reasonable grounds to believe that this individual would engage in activities constituting a threat to the security of Canada.

At the hearing, evidence was heard from CSIS to the effect that the activities of this individual were in keeping with those of an agent of a foreign government.

The Presiding Committee Member proposed to disclose certain allegations to the applicant and counsel so a reasonable defence could be mounted. The Presiding Committee Member did not seek to disclose facts prejudicial to national security but insisted on appropriate disclosure as required by law.

CSIS then informed the Secretary of State that it wished to withdraw its objection to citizenship for this individual.

The Presiding Committee Member ended the investigation as there was no longer any basis for continuing.

4. An individual who found refuge in Canada after a military coup and later gained landed immigrant status was denied citizenship when CSIS said this individual was a sympathizer of a terrorist organization in the country of origin.

Paragraph 2(*c*) of the *CSIS Act* provides that "threats to the security of Canada" include

> activities within ... Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada *or a foreign state*. (emphasis added)

Both the applicant and CSIS were assisted by counsel at the hearings, and both presented evidence. The Presiding Committee Member also called an expert witness to fill in the background about terrorist organizations in the country of the applicant's origin.

The Presiding Committee Member concluded that this individual did not threaten the security of Canada, and recommended that citizenship be granted.

At the time of writing, the report of the Presiding Committee Member had not yet been acted upon by the Governor in Council.

5. This case, while it was the subject of a separate report, involves the spouse of the applicant dealt with in the preceding case history. The facts and the recommendation are the same. At the time of writing, the report of the Presiding Committee Member had not yet been acted upon by the Governor in Council.

6. Citizenship was denied to a landed immigrant, in Canada since 1966, because CSIS believed that this individual was a threat to the security of Canada. Before the Committee began its investigation, CSIS withdrew its recommendation against granting citizenship.

7. An individual who entered Canada as a refugee and was granted landed immigrant status more than a decade ago was refused citizenship when CSIS alleged that this individual was an agent of influence for a foreign intelligence service. CSIS withdrew its objections to citizenship for this individual before the Committee completed its investigation.

Immigration

8. Upon entering Canada, an individual was detained by immigration authorities, then released the following day after an appearance before an immigration adjudicator.

The Solicitor General and the Minister of Employment and Immigration subsequently reported to the Committee that this individual met the criteria for deportation under the *Immigration Act, 1976*. The specific allegations were to the effect that this person had a close and active association with a terrorist organization and was known to have engaged in terrorist acts.

At the hearing, CSIS supported these allegations. Evidence by the applicant and by witnesses in support of the applicant lacked credibility.

The Presiding Committee Member concluded that that there were reasonable grounds to believe that this person would instigate the subversion by force of the democratic government of another country while in Canada, and recommended that deportation proceedings be instituted.

At the time of writing, the Presiding Committee Member's report had not yet been acted upon by the Governor in Council but the applicant left the country.

Appendix C

SIRC Staff on April 1, 1987

Maurice Archdeacon, Executive Secretary	990-6839
Yvette Collins, Senior Secretary	990-8442
Danielle Blache, Secretary	991-9112
Annie Demirjian, Executive Assistant	990-6319
Shirley Heafey, Senior Complaints Officer	993-4263
Arthur Graham, Director of Research*	990-8051
Maurice M. Klein, Research Officer	990-8445
John M. Smith, Research Officer	991-9111
Joan Keane, Research Assistant	990-8443
Madeleine DeCarufel, Administration Officer and Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, Records Clerk	998-5258
Diane Marion, Receptionist-Secretary	990-8441

* Throughout 1986-87, the Director of Research was Jacques J.M. Shore, who resigned on March 31, 1987, to practice law in Montreal. We wish to record our gratitude for the contribution he made in the two years he was with us.

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Rapport annuel

1986-1987

© Ministre des Approvisionnements et Services Canada 1987

N° de cat. JS71-1/1987

ISBN 0-662-55252-0

Comité de surveillance des activités
de renseignement de sécurité
14e étage
365, avenue Laurier ouest
C.P. 2430, Succursale D
Ottawa (Ontario)
K1P 5W5

(613) 990-8441 — Les appels à frais virés sont acceptés et le standard téléphonique est ouvert de 7 h 30 à 18 h, heure d'Ottawa.

La citation de *The RCMP and the Management of National Security* paraît avec la permission de l'Institut de recherches politiques.

Le 22 juin 1987

L'honorable James F. Kelleher, C.P., député, c.r.
Solliciteur général du Canada
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Monsieur le Ministre,

Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous soumettons au Parlement, par votre intermédiaire, le rapport annuel du Comité de surveillance des activités de renseignement de sécurité pour l'année financière 1986-1987.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Le président,

Ronald G. Atkey, C.P., C.R.

Jean Jacques Blais, C.P., C.R.

Frank McGee, C.P.

Saul M. Cherniack, C.P., C.R.

Paule Gauthier, C.P.

Quis cusodiet ipsos custodes?

(Qui gardera les gardiens eux-mêmes?)

Juvenal

Table des matières

1. **Introduction** 1

Mandat 1
Relations avec le SCRS 2
Notre façon de procéder 3
Pour mémoire 3
Équilibre 4

2. **Contrôle** 5

Contrôles officiels 5
Indications ministérielles 6
Rapport annuel du SCRS et certificat de l'inspecteur général 7
Le processus de contrôle 7

3. **Comment le SCRS acquiert ses renseignements** 11

Dossiers des mandats judiciaires de la Cour fédérale 11
Données statistiques 12
Le courrier des autres 13
Mandats judiciaires d'urgence 14
Sources ouvertes 15
Centre d'information de la police canadienne 17
Les universités et le gouvernement 18
Ententes entre organisations au Canada 19
Ententes avec l'étranger 20
Actes illégaux 22

4. **Ce que sait le SCRS** 25

Limites légales 25
Information héritée 25
Fermeture des vieux dossiers 27
Renseignements étrangers 27
Information indirecte 28

5. **Ce que fait le SCRS** 29

Information indirecte qui pourrait être utile 29
Le SCRS en cour 29
Aide à la police 30
Relations avec la GRC 31
Alerte à l'aéroport 32
Agents de liaison avec l'étranger 34
Persona non grata 34
L'intérêt public 34
Organismes de façade 34

6. Opérations d'antisubversion 37

Les principes et la loi 37
Notre façon de procéder 38
Transition 38
Ressources 39
Sources humaines 39
Ciblage 40
Dossiers sur des particuliers 42
Diffusion de l'information 43
Cinq organismes 44
Deux champs d'action 45

7. Le SCRS lui-même 47

Ressources et administration 47
Transformation en organisme civil 48
Provenance des recrues 49
L'Académie ferme ses portes 50
Bilinguisme et participation équitable 51
La première classe 52
Amélioration du moral 53
Utilisation du polygraphe 53

8. Combler les fossés 57

Langues officielles 57
Relations de travail 60

9. Plaintes 63

Un bon point pour la défense 63
Habilitations de sécurité 63
Plaintes contre le SCRS 64
Immigration et citoyenneté 65
Qualité des enquêtes 66
Étude concernant la Loi sur l'immigration 67
La nouvelle politique de sécurité 68

10. Précisions diverses 73

Comptes rendus au Parlement 73
Sensibilisation 73
Réunions et conférences 73
Personnel 74
Rapport financier 75

11. Projets d'avenir 77

Examen quinquennal 77
La portée du contrôle 78
Un dernier mot 79

Annexes

A: Directives ministérielles, 1986-1987 81
B: Résumés des causes 83
C: Personnel du CSARS 87

1. Introduction

L'examen indépendant et externe du renseignement de sécurité est un phénomène récent dans toutes les démocraties. Ici au Canada, il ne remonte qu'à 1984, année où le Parlement a adopté la *Loi sur le Service canadien du renseignement de sécurité (Loi sur le SCRS)*.

En vertu de cette loi, les responsabilités du service de sécurité de la GRC ont été transférées au nouveau Service canadien du renseignement de sécurité (SCRS). Notre Comité, le Comité de surveillance des activités de renseignement de sécurité (CSARS) et un inspecteur général ont été nommés et chargés respectivement du contrôle externe et du contrôle interne. L'inspecteur général fait rapport au solliciteur général.

Pionniers dans un nouveau secteur de l'administration publique, nous avons d'abord été obligés de nous faire la main. Ce défi était manifeste dans nos deux premiers rapports annuels.

Cependant, au moment d'entamer la deuxième moitié de notre mandat quinquennal, nous commençons à régler notre tir. Nous sommes maintenant équipés pour analyser les statistiques sur les opérations du SCRS et repérer les tendances. Nous avons également effectué des études majeures—sur l'antisubversion, par exemple—tout en donnant suite à des dizaines de questions au moyen de demandes d'information écrites et d'entrevues avec les agents du SCRS.

Nous suivons le cap fixé. Nous espérons que les lecteurs du présent rapport annuel penseront comme nous qu'à l'heure actuelle l'examen externe suit fidèlement le cap fixé. Nous abordons plus de sujets et nous les traitons plus en profondeur que dans nos deux derniers rapports.

Nous reprenons certains thèmes des années passées. Par exemple, nous croyons fermement que le SCRS n'a pas suffisamment recours aux sources ouvertes comme solution de rechange aux enquêtes clandestines. Nous continuons également de donner un compte rendu du nombre total de mandats judiciaires, nouveaux et renouvelés, que la Cour fédérale du Canada accorde au SCRS.

Parmi les sujets que nous avons examinés plus en profondeur figurent le programme d'antisubversion, et particulièrement la façon dont les cibles sont choisies, les relations entre le SCRS et la GRC dans les opérations d'antiterrorisme, et la transformation en organisme civil.

Nous craignons de plus en plus que la transformation en organisme civil n'avance trop lentement parce que le recrutement est fortement axé sur d'anciens policiers. Cela ne peut que perpétuer l'approche policière que le Parlement avait l'intention de changer en adoptant la *Loi sur le SCRS*.

Mandat

En termes généraux, nous sommes mandatés pour voir à ce que le Service effectue son travail efficacement mais sans empiéter déraisonnablement ni inutilement sur les droits indi-

viduels. Les tâches spécifiques que nous confère la *Loi sur le SCRS* se divisent en deux grandes catégories : le contrôle et les plaintes.

Contrôle. L'alinéa 38a) de la *Loi sur le SCRS* nous charge de «surveiller la façon dont le Service exerce ses fonctions», alors que l'alinéa 38b) et l'article 40 nous permettent «d'effectuer ou de faire effectuer des recherches» afin de «veiller à ce que les activités du Service soient conduites conformément à la présente loi, à ses règlements et aux instructions du ministre ... et qu'elles ne donnent pas lieu à l'exercice par le Service de ses pouvoirs d'une façon abusive ou inutile».

Les chapitres 2 à 8 du présent rapport décrivent ce que nous avons fait l'an passé pour remplir notre mandat à l'égard du contrôle.

Le contrôle ne signifie pas que nous sommes un genre de conseil d'administration pour le SCRS. Nous n'hésitons pas à donner des conseils, privément lorsque les circonstances le dictent et en public lorsque nous le pouvons, par le truchement de nos rapports annuels et de témoignages devant les comités parlementaires.

Mais nous ne pouvons formuler de politiques ni donner d'ordres. Et nous ne voudrions pas le faire, parce que nous deviendrions alors des intervenants actifs dans le secteur du renseignement de sécurité et que nous perdrions ainsi la liberté de critiquer qui est notre raison d'être.

Plaintes. En vertu de l'alinéa 38c), nous sommes tenus de faire enquête sur les plaintes portées par toute personne concernant des activités du Service ou le refus d'une habilitation de sécurité requise pour un emploi dans la Fonction publique ou pour la fourniture de biens ou de services au gouvernement fédéral. Nous enquêtons aussi sur les questions touchant la citoyenneté et l'immigration et sur les aspects de sécurité de certaines plaintes portées auprès de la Commission canadienne des droits de la personne.

Le chapitre 9 du présent rapport traite de notre travail dans ce domaine, et des résumés des causes figurent à l'Annexe B.

Relations avec le SCRS

Des relations à distance avec le SCRS et d'autres participants dans le secteur canadien du renseignement de sécurité sont le prix de notre indépendance.

La rançon des vastes pouvoirs du SCRS est un contrôle indépendant externe.

Le Service nous fournit l'information que nous demandons, mais il reste distant et méfiant. Cela n'est pas nécessairement mauvais; nous aurions du mal à maintenir notre indépendance si nos liens avec le Service étaient trop étroits.

Notre façon de procéder

La *Loi sur le SCRS* prévoit que les membres de notre Comité devront être nommés par le gouverneur en conseil après consultation du Premier ministre avec le chef de l'opposition et les chefs de chaque parti comptant douze membres ou plus à la Chambre des communes.

En faisant les nominations initiales, le Premier ministre a donné à ces consultations une très vaste envergure : il a invité le chef de l'opposition et le chef du Nouveau parti démocratique à nommer un membre chacun et il a lui-même nommé trois membres. L'effectif du Comité a ensuite été soumis à l'approbation des trois dirigeants. Par conséquent, notre Comité est clairement tripartite.

Une fois le processus de nomination terminé toutefois, nous avons jugé souhaitable de laisser les considérations partisanes à la porte. Le plus souvent, nous remplissons notre rôle à l'égard du contrôle collégialement, par consensus. De plus, le fait que nous sommes des membres à temps partiel, actifs dans nos collectivités et dans la vie privée à l'extérieur des cercles gouvernementaux à Ottawa, nous permet de mieux nous concentrer sur notre tâche d'une façon non partisane lorsque nous nous réunissons.

Les plaintes sont habituellement entendues par un seul membre du Comité. Les rapports finals sont revus par tous, mais nous fournissons des opinions juridiques et des commentaires seulement. Nous ne cherchons pas à discuter ni à modifier le raisonnement ou les conclusions, en partant du principe que c'est seulement la personne qui a entendu la preuve en premier lieu qui peut donner à chaque élément de la cause le poids qui lui revient. En vertu de nos règles sur les conflits d'intérêts, les membres du Comité ne participent pas du tout aux affaires s'ils ont préalablement une connaissance du particulier concerné ou eu des rapports avec lui.

Pour mémoire

Lorsque nous avons choisi la citation bien connue de Juvenal «Qui gardera les gardiens eux-mêmes?» comme l'épigraphe du présent rapport, nous songions à nos rapports avec le SCRS, certes. Mais nous songions également à nous-mêmes. Le Parlement et les Canadiens doivent dans une grande mesure compter sur notre Comité et sur l'inspecteur général pour garantir que les droits et libertés individuels sont protégés dans le secteur du renseignement de sécurité.

C'est pourquoi, en rédigeant notre rapport annuel, nous essayons de citer publiquement autant de faits que possible. Plus nous en disons, mieux le Parlement et les Canadiens seront en état de juger eux-mêmes.

Nous sommes, de toute évidence, restraints par la disposition légale qui nous interdit de ne rien révéler qui compromettrait la sécurité nationale. En vertu de la *Loi*, le SCRS revoit le projet de rapport et nous prévient de toute information qu'il juge compromettante. Certains détails à l'appui de l'information sont omis du rapport publié par suite de ce processus, mais nous croyons que rien de vraiment important n'est perdu.

Équilibre

Les rapports annuels des organismes de contrôle ou de vérification fournissent habituellement une kyrielle de critiques plutôt qu'un tableau équilibré. Cela est normal.

En outre, notre rapport annuel est limité par notre incapacité de commenter les succès du SCRS, pour des raisons de sécurité nationale. Il y a eu nombre de succès, particulièrement dans les domaines du contre-espionnage et de l'antiterrorisme.

Ce rapport ne donne donc qu'une vue partielle, comme celle que l'on aurait d'une porte entrouverte. Si nous pouvions ouvrir toute grande cette porte, nous inclurions beaucoup plus d'informations sur le travail important et effectif accompli jour après jour par le Service. C'est une institution nationale importante qui mérite l'appui continu du public.

Nous sommes frappés par le dévouement et le professionnalisme des employés du SCRS chaque fois que nous entrons en contact avec eux d'une extrémité à l'autre du pays.

2. Contrôle

Le SCRS protège-t-il l'intérêt national aussi effectivement que possible? Est-il efficace—tant en regard des objectifs administratifs comme l'intégrité financière que des objectifs d'orientation comme la transformation en organisme civil et le bilinguisme officiel? Donne-t-il suffisamment de poids aux droits et libertés individuels?

Réduit à sa plus simple expression, notre mandat à l'égard du contrôle consiste à suivre ces questions au nom du Parlement et du peuple canadien. Notre rôle particulier est de surveiller l'équilibre délicat entre la sécurité nationale et les libertés individuelles.

Le contrôle fait l'objet du présent chapitre et des six qui suivent. Nous commençons par étudier les contrôles officiels exercés sur le SCRS. Nous traitons ensuite de diverses questions regroupées sous trois rubriques générales : la collecte de l'information, la gestion de l'information et l'utilisation de l'information. Comme une étude approfondie que nous avons effectuée du programme d'antisubversion du SCRS englobe tous ces thèmes, nous lui consacrons son propre chapitre. Nous terminons notre rapport par un examen de certaines questions touchant la gestion interne et par un chapitre sur une étude d'envergure que nous avons entreprise, à la demande du solliciteur général, sur les langues officielles et les relations de travail au SCRS.

Contrôles officiels

À cause de ses vastes pouvoirs d'enquête et de la nature inévitablement secrète d'une grande partie de son travail, le SCRS est assujetti à une gamme de contrôles, aussi bien judiciaires qu'administratifs.

Avant d'exercer ses plus vastes pouvoirs comportant intrusion, il doit convaincre un juge de la Cour fédérale du Canada de délivrer un mandat judiciaire (Partie II de la *Loi sur le SCRS*). En fait, il doit d'abord obtenir l'approbation du ministre.

Le SCRS doit obtenir le consentement personnel du solliciteur général dans un certain nombre d'autres circonstances—avant de conclure une entente avec une province, par exemple (article 17 de la *Loi*).

En outre, le solliciteur général peut donner des instructions au SCRS concernant la conduite d'une affaire particulière ou de toutes classes d'affaires (paragraphe 6(2) de la *Loi*).

Le solliciteur général a, en l'inspecteur général, son propre agent de surveillance du SCRS (articles 30 à 33 de la *Loi*). L'inspecteur général délivre un certificat annuel indiquant s'il est satisfait du rapport annuel secret que le directeur du SCRS remet au solliciteur général, si le Service s'est conformé à la *Loi* et aux indications du solliciteur général dans la conduite de ses activités opérationnelles, et s'il a exercé ses pouvoirs de façon déraisonnable ou inutile.

Notre mandat comporte tous ces contrôles (article 38 de la *Loi sur le SCRS*). Nous examinons les indications du solliciteur général, le rapport annuel du directeur et le certificat de l'inspecteur général, et nous avons l'oeil sur les mandats judiciaires.

Les mandats judiciaires sont traités dans le prochain chapitre. Nous faisons ci-dessous de brèves observations sur les autres contrôles officiels.

Indications ministérielles

Le solliciteur général donne deux genres d'indications, à savoir les directives ministérielles et les instructions ministérielles. Les directives sont des déclarations de principe qui précisent comment doivent être traitées les opérations d'une classe donnée. Elles exigent habituellement le renvoi de certaines questions au solliciteur général pour qu'il les tranche individuellement.

D'autre part, l'instruction prend habituellement la forme d'une correspondance qui touche une affaire particulière et dans laquelle le solliciteur général peut incidemment fournir des conseils d'orientation ou établir des précédents applicables à d'autres cas.

Dans le rapport annuel de l'an dernier, nous avons indiqué que, après avoir examiné le compendium des instructions ministérielles renfermant toutes les directives et instructions connues données à l'ancien service de sécurité de la GRC et au SCRS, nous avions posé un certain nombre de questions qui restaient sans réponse. Nous sommes satisfaits des réponses que le SCRS et le ministère du Solliciteur général nous ont données depuis lors.

Nous avons également affirmé l'an dernier que le SCRS revoyait le compendium à la recherche d'éléments qu'il devrait peut-être modifier pour les rendre conformes à la *Loi sur le SCRS*. Nous croyons comprendre que cette tâche est maintenant presque terminée, et il nous presse d'en connaître les résultats.

Nouvelles questions. Nous avons reçu copie de neuf nouvelles directives et instructions en 1986-1987. Une liste se trouve à l'Annexe A du présent rapport. À la fin de mars, nous en avons reçu deux que nous n'avons pas eu l'occasion d'examiner pendant l'année financière sous étude. Quant à celles que nous avons pu étudier, nous sommes persuadés qu'elles ne comportent aucun exercice déraisonnable ni inutile des pouvoirs du Service ni n'empiètent indûment sur les droits individuels ou la vie privée.

Le solliciteur général nous a aussi informés en 1986-1987 que sept directives et instructions avaient été retirées. Une indication portait sur les évaluations de sécurité et a été remplacée par de nouvelles indications. Quant aux autres, elles étaient périmées.

Dans le cadre de notre examen des statistiques relatives aux activités opérationnelles, nous surveillons maintenant le nombre d'opérations approuvées au moyen d'une directive ministérielle. Cela mettra en lumière tout changement de taille que nous devrons examiner plus en profondeur.

Nous pouvons dire d'ores et déjà que les opérations délicates au point d'exiger l'autorisation explicite du ministre ne sont pas nombreuses.

Cependant, nous avons découvert en 1986-1987 que nous ne recevions pas copie de tous les documents que nous considérons comme des directives ou des instructions ministérielles.

Le problème résidait dans l'interprétation étroite qui était donnée au statut légal de ces indications.

À notre demande, le SCRS revoit toute sa correspondance avec le solliciteur général afin que les lacunes de nos dossiers puissent être comblées et que nous ne soyons pas confrontés de nouveau au même problème.

Rapport annuel du SCRS et certificat de l'inspecteur général

Nous avons examiné à la fois le rapport annuel du directeur au solliciteur général et le certificat de l'inspecteur général pour l'année civile 1986 et sommes convaincus qu'ils donnent un aperçu réaliste du travail du Service.

À cause de leur cote—secret dans le cas du rapport annuel et très secret dans celui du certificat—nous ne pouvons divulguer leur contenu.

Toutefois, les informations qu'ils renferment étayent les observations que nous faisons de notre propre chef dans le présent rapport et aideront à guider nos activités de contrôle faites sur une base continue.

Nous profitons de cette occasion pour remercier l'inspecteur général pour son énergie, son industrie et sa minutie.

Le processus de contrôle

Pour conclure ce chapitre, nous donnons quelques faits au sujet de nos opérations de contrôle en général.

Ère de l'informatique. En 1986-1987, nous sommes entrés dans l'ère de l'informatique en acquérant la capacité matérielle dont nous avons besoin pour remplir notre mandat consistant à «réunir et analyser des statistiques sur les activités opérationnelles du Service» (sous-alinéa 38a)(vii) de la *Loi sur le SCRS*).

Des raisons de sécurité limitent strictement ce que nous pouvons dire au sujet des conclusions que nous tirons de l'analyse statistique.

Cependant, nous avons poursuivi notre pratique consistant à fournir des statistiques sur les mandats judiciaires (page 12 du présent rapport). L'analyse statistique sous-tend également un grand nombre de nos observations concernant la mesure où le SCRS a eu recours à divers instruments d'enquête, son budget et ses dépenses, l'incidence de la *Loi sur le SCRS* sur les opérations, et les progrès accomplis vers la transformation en organisme civil.

La valeur de l'analyse statistique est qu'elle nous permet de poser des questions pertinentes au SCRS sans être obligés d'examiner chaque opération, ce qui serait une tâche impossible.

Des statistiques ont été obtenues du SCRS touchant l'allocation des ressources, les mandats judiciaires, l'utilisation des sources, les opérations aux campus, le personnel, le ciblage de groupes et de particuliers aux fins d'enquête, les actes illégaux et d'autres questions. La plupart des données sont fournies sur une base trimestrielle.

Dans la majorité des domaines, nous avions des données pour seulement un trimestre de 1986-1987, ce qui a nécessairement limité notre travail analytique. Il était, de toute évidence, impossible de déterminer les tendances dans ces cas. À mesure que nous accumulons plus d'informations, nous nous attendons à ce que l'analyse statistique constitue un outil de contrôle important.

Aucune des données que nous avons vues ne laissait supposer que le Service exerce ses pouvoirs de façon déraisonnable ou inutile.

Demandes d'information officielles. Nous transmettons par écrit au SCRS des demandes d'information officielles. Des 145 que nous avons présentées en 1986-1987, seulement 18 demeuraient sans réponse à la fin de l'année.

Nous tirons nos questions de nombreuses sources. Certaines émanent évidemment de notre propre recherche et d'autres, de nos enquêtes sur des plaintes.

D'autres questions encore nous sont suggérées par des bulletins de nouvelles—par exemple, en 1986-1987, des reportages concernant la collecte de fonds alléguée pour les rebelles Contra au Nicaragua, le recrutement par la Nation Aryenne prônant la suprématie de la race blanche, la surveillance alléguée d'un militant pour la paix qui a rencontré une personne soupçonnée d'être un agent soviétique, les demandes d'immigration présentées par des personnes qui seraient coupables de torture et de meurtres au Chili, et bien d'autres.

Nous avons suivi l'enquête sur le désastre d'Air India survenu le 23 juin 1985. Il n'y a malheureusement rien que nous pouvons dévoiler publiquement. Nous pouvons seulement promettre de rester attentifs à l'enquête qui se poursuit.

Nous examinons aussi avec le SCRS les questions posées par les membres de comités parlementaires au directeur et auxquelles il ne peut répondre devant des instances aussi publiques. Certaines des questions qui ont été soulevées lorsque le Comité permanent de la Chambre des communes chargé de la justice et du solliciteur général a questionné le directeur le 11 décembre 1986 ont reçu une réponse qui nous satisfait; nous attendons les réactions à d'autres.

Séances d'information. Nous nous sommes réunis en comité avec le solliciteur général, et le président a tenu des rencontres fréquentes avec le solliciteur général, le sous-solliciteur général, le directeur du SCRS et l'inspecteur général.

Profitant des réunions que nous ne manquons pas de tenir régulièrement dans différentes villes du Canada, nous visitons les bureaux locaux du SCRS pour y rencontrer la direction et le personnel et nous renseigner sur les opérations de ces régions. En 1986-1987, nous avons visité la région d'Ottawa, la région des Prairies à Edmonton, la région de l'Atlantique à Halifax, la région du Québec à Montréal et la région de Toronto.

Notre visite à Montréal est survenue en novembre, aux dernières étapes de notre étude spéciale sur les langues officielles et les relations de travail au SCRS (prévue au chapitre 8). Nos discussions avec les gestionnaires aussi bien que le personnel là-bas nous ont aidé à mieux comprendre la situation au moment de rédiger notre rapport sur cette enquête.

3. Comment le SCRS acquiert ses renseignements

Ce chapitre examine la collecte d'informations par le SCRS et certaines questions qu'elle a soulevées.

Dossiers des mandats judiciaires de la Cour fédérale

Pour exercer ses plus vastes pouvoirs comportant intrusion, le SCRS doit obtenir un mandat judiciaire d'un juge de la Cour fédérale du Canada. Ces pouvoirs comprennent l'écoute électronique, l'écoute par microphone, l'interception d'images optiques, l'interception de communications enregistrées, les perquisitions en vue de trouver documentation et objets et l'interception du courrier.

Bien que nous n'y soyons pas tenus par la loi, nous lisons certains affidavits faits sous serment à l'appui des demandes de mandats judiciaires.

Mais les affidavits ont déjà été vus par le solliciteur général aussi bien que par des juges de la Cour fédérale du Canada avant de nous parvenir. Nous avons donc décidé d'aller plus loin et d'examiner les dossiers opérationnels sur lesquels ils s'appuient.

Comme ces dossiers ne sont vus par personne d'autre que l'inspecteur général et nous à l'extérieur du Service, notre examen fournit une deuxième ligne de protection distincte contre l'exercice déraisonnable ou inutile par le SCRS de ses pouvoirs.

Nous avons déterminé que les affidavits étaient généralement factuels mais, chose qui n'est pas surprenante, qu'ils tendaient à justifier l'utilisation des techniques comportant intrusion plutôt qu'à faire un exposé équilibré de leurs avantages et inconvénients.

L'avocat du diable. Lorsque le SCRS demande un mandat judiciaire, il n'y a évidemment pas de représentant pour la cible.

Nous avons été informés que le solliciteur général s'assure, en examinant les demandes de mandats judiciaires, que tous les faits qui sont attestés sous serment sont vérifiables, et qu'il ne s'agit pas seulement de conclusions que l'enquêteur a tirées des faits. Il lui arrive de renvoyer certaines demandes pour qu'elles soient modifiées avant d'être transmises à la Cour fédérale. En réalité, nous avons appris qu'il avait carrément rejeté des demandes. Nous applaudissons à sa vigilance.

Nous reconnaissons aussi le rôle joué par les juges de la Cour fédérale qui entendent chaque affaire. La Cour n'a rejeté aucune demande, mais les juges ont demandé, dans certains cas, des éclaircissements et ont imposé dans l'ordonnance accordant le mandat des conditions destinées à protéger les droits individuels (voir, par exemple, la page 23 du présent rapport).

Mais aucun des contrôles actuellement exercés par le solliciteur général et par les juges n'est plus fort que l'engagement personnel des particuliers concernés. Pour notre part, notre examen est effectué après coup; nous pourrions prévenir le Parlement si jamais il y avait abus flagrant, mais il serait trop tard pour y faire obstacle.

Le solliciteur général, conjointement avec le SCRS, devrait se demander s'il y aurait lieu de prévoir à une étape de la procédure — soit devant la Cour fédérale ou devant le solliciteur général lui-même — un «avocat du diable» qui présenterait les arguments militant contre la délivrance du mandat.

Le Parlement pourrait aussi envisager cette possibilité pendant l'examen quinquennal de la *Loi sur le SCRS* en 1989.

Clauses omnibus. Les cibles sont généralement nommées dans les mandats judiciaires. L'endroit où un mandat judiciaire peut être exercé est précisé. Les «Clauses omnibus» permettent l'exercice des pouvoirs comportant intrusion au même endroit à l'égard des associés de la cible, lesquels peuvent être nommés seulement après la délivrance du mandat. En l'absence de telles clauses, le SCRS serait obligé de demander un nouveau mandat à la Cour fédérale chaque fois qu'un associé de la cible apparaît.

L'inspecteur général étudie actuellement la question de savoir qui peut désigner des cibles en vertu des «clauses omnibus» dans les mandats judiciaires.

L'utilisation des clauses omnibus nous inquiète aussi. En premier lieu, nous aimerions savoir si ces clauses sont même acceptables. Le cas échéant, il faudra déterminer qui au sein du SCRS—ou du ministère du Solliciteur général—devrait avoir le pouvoir de désigner des cibles additionnelles qui ne sont pas nommées dans le mandat judiciaire.

Données statistiques

Dans le cadre de nos fonctions de contrôle, nous avons commencé à réunir des statistiques trimestrielles sur les mandats judiciaires. Notre nouveau matériel informatique nous permet maintenant d'examiner l'utilisation des mandats judiciaires dans l'ensemble et selon le type de pouvoirs, de régions ou de cibles. Les données d'ensemble pour les années civiles 1985 et 1986 figurent au Tableau 1.

Tableau 1. Mandats judiciaires nouveaux et renouvelés délivrés au SCRS, 1985 et 1986

	1985	1986
Nouveaux mandats	82	94
Mandats renouvelés	27	11
Total	109	105
Durée moyenne des mandats judiciaires (jours)	173,6	162,2

(Source : SCRS)

Les données brutes que nous fournissons ici ne permettent aucune comparaison probante avec les statistiques antérieures à 1985 sur les mandats judiciaires.

Avant le 16 juillet 1984, date d'entrée en vigueur de la *Loi sur le SCRS*, les mandats judiciaires en vue des enquêtes dans le secteur du renseignement de sécurité étaient délivrés en vertu de la *Loi sur les secrets officiels*. Chacun de ces mandats permettait normalement l'exercice d'un pouvoir à l'égard d'une cible.

La portée des mandats judiciaires délivrés depuis lors en vertu de la *Loi sur le SCRS* peut être beaucoup plus vaste. Un de ces mandats peut autoriser l'exercice d'un grand nombre de pouvoirs à l'égard d'un grand nombre de cibles.

Maximum. Nous discutons avec le SCRS des meilleures façons de présenter le plus grand nombre d'informations au public concernant les mandats judiciaires et l'utilisation des pouvoirs comportant intrusion.

Nous continuons de craindre que les statistiques d'ensemble sur les mandats judiciaires délivrés en vertu de la *Loi sur le SCRS* ne brossent pas un tableau aussi exact du niveau des activités comportant intrusion que les statistiques qui étaient publiées en vertu de la *Loi sur les secrets officiels*.

Nous obtenons suffisamment d'informations du SCRS pour pouvoir élaborer nous-mêmes des statistiques plus révélatrices et les publier. Mais, sans preuve d'abus, nous respectons la position du Service à l'effet que des renseignements fort valables pour la sécurité seraient divulgués si les faits complets étaient révélés.

Il s'agit là d'une autre question que le Parlement pourrait vouloir soulever au moment de l'examen quinquennal de la *Loi sur le SCRS* en 1989.

Le courrier des autres

Nous avons fait une étude particulière de l'ouverture du courrier. Après le tollé que l'ouverture illicite du courrier par la GRC a suscité il y a quelques années, certains Canadiens étaient inquiets lorsque le SCRS a obtenu le pouvoir légal d'intercepter le courrier, même si ce pouvoir était sujet aux mêmes exigences touchant les mandats judiciaires que toute autre activité comportant intrusion.

Ils ont peut-être imaginé des escouades d'hommes et de femmes en trench-coat et en chapeaux mous, penchés sur des bouilloires, décachetant à la vapeur des lettres à tante Marie et enregistrant solennellement des potins familiaux.

Notre impression était tout à fait différente. Mis à part le fait que des méthodes d'une haute technicité ont remplacé les bouilloires, à la fin de 1986, le SCRS avait ouvert très peu d'enveloppes.

Nous avons des raisons de croire que l'interception du courrier augmentera. Seulement des difficultés techniques ont empêché le Service d'intercepter le courrier de deux autres cibles en 1986. Au début de 1987, le SCRS détenait quelques mandats judiciaires accordant des pouvoirs d'ouverture du courrier qu'il était prêt à exercer selon les besoins. Un seul mandat judiciaire peut toucher plus d'une adresse.

Le SCRS affirme qu'il a l'intention de recourir à ce pouvoir seulement lorsqu'il est justifié de soupçonner qu'un particulier ou un organisme se sert du courrier pour donner suite à une menace envers la sécurité nationale.

Nous continuerons de réviser l'ouverture du courrier.

Postes Canada collabore avec le SCRS à cet égard et un protocole d'entente officiel entre les deux organismes est en voie de rédaction. Il sera soumis à notre examen en temps opportun.

Nous aimerions voir des modalités de collaboration comportant moins d'intrusion que l'interception du courrier. Prenons l'exemple du dépistage. Postes Canada est en mesure de fournir au SCRS des listes donnant les nom et adresse des correspondants d'une cible. Il faudrait déterminer si ces listes devraient également faire l'objet d'un mandat judiciaire.

Mandats judiciaires d'urgence

Avant de terminer notre étude de l'utilisation des pouvoirs comportant intrusion, nous soulevons encore une fois la question des mandats judiciaires d'urgence.

Les demandes de mandats judiciaires sont habituellement présentées par un enquêteur. Les agents supérieurs et un comité officiel d'examen des mandats judiciaires procèdent alors à un examen interne. En vertu de la *Loi sur le SCRS*, toutes les demandes doivent être personnellement approuvées par le solliciteur général avant d'être soumises à un juge de la Cour fédérale.

Aussi encombrante qu'elle puisse paraître, cette procédure a été suffisamment simplifiée pour permettre au SCRS d'obtenir à temps tous les mandats dont il a eu besoin. Mais, tôt ou tard, une opération sera inévitablement affaiblie parce qu'un mandat judiciaire n'aura pu être obtenu assez rapidement.

Cela pourrait-il arriver? Nous avons exposé dans notre dernier rapport annuel un scénario dans lequel le SCRS apprend à la dernière minute qu'un terroriste fera escale à un aéroport canadien. Un mandat instantané permettrait de surveiller toute réunion tenue par ce dernier pendant le battement. Voilà un genre de cas où les procédures actuelles pourraient être trop lentes.

Nous avons indiqué que la *Loi* pourrait être modifiée de façon à ce que le directeur du SCRS puisse lui-même délivrer en cas d'urgence un mandat qui serait rapidement examiné—à l'intérieur de 48 heures, disons—par un juge de la Cour fédérale. Nous avons aussi suggéré qu'un rapport préliminaire soit présenté au solliciteur général et à nous-mêmes.

Nous estimons toujours que des circonstances spéciales exigent des mesures spéciales et que des procédures visant la délivrance de mandats judiciaires en cas d'urgence devraient être incorporées dans la *Loi*.

Pour aider le Parlement au moment de l'examen quinquennal de la *Loi* en 1989, nous avons commencé à réunir des statistiques sur le délai d'obtention des mandats judiciaires. Ces statistiques pourraient faire ressortir tout goulet d'étranglement du système et étayer le besoin de mesures spéciales.

Sources ouvertes

Le SCRS peut limiter l'exercice de ses pouvoirs comportant intrusion en faisant appel à des sources ouvertes comme les périodiques érudits et les mass médias, tant à l'étranger qu'au Canada.

Nous sommes loins d'être persuadés que le SCRS prend les sources ouvertes suffisamment au sérieux comme solutions de rechange au travail d'infiltration. L'utilisation des sources ouvertes reste une pâle imitation de ce qu'envisageait la Commission McDonald et de ce que nous avons vivement recommandé à maintes reprises pour assurer à la fois l'efficacité des opérations de renseignement de sécurité et un minimum d'intrusion dans la vie privée et les libertés personnelles.

Nous reconnaissons que le Service a commencé à créer des sections de référence dans les bureaux régionaux en 1986-1987 et qu'il a élargi la Section de l'information de sources ouvertes à l'Administration centrale.

Cette section compte maintenant une section des services techniques, un service de recherche, un Centre des opérations d'urgence et deux services de référence. Un comité d'utilisateurs a été mis sur pied afin d'aider la Section à se tenir au courant des besoins réels du Service, et des employés supplémentaires ont été nommés. Certaines vacances subsistent, mais on a pourvu aux postes clés.

Service bilingue. En particulier, nous sommes heureux que la Section de l'information de sources ouvertes compte maintenant davantage d'employés bilingues et qu'elle prévoit de porter de un à trois le nombre de bases de données en langue française auxquelles elle a actuellement accès.

Comme nous le notons ailleurs dans le présent rapport (chapitre 8), le Service a beaucoup tardé à fournir à ses employés francophones et anglophones une façon égale de travailler dans leur propre langue, et nous nous réjouissons de tous les progrès qui sont accomplis vers cet objectif.

Cependant, les services fournis en français sont toujours nettement inférieurs à ceux qui sont fournis en anglais, et nous encourageons la mise à exécution dans les plus brefs délais possibles des plans visant à augmenter les renseignements et les services qui sont accessibles en français. En particulier, nous espérons qu'un recours accru aux médias étrangers de sources ouvertes en langue française s'ensuivra.

Recherche. En général, nous croyons que le Service ne profite pas pleinement des occasions qui lui sont offertes d'utiliser les sources ouvertes.

Le service de recherche nous préoccupe énormément. Dans notre dernier rapport annuel, nous affirmions que le Service avait préféré choisir ses recherchistes parmi ses agents de renseignements ayant une longue expérience pratique, et nous avons indiqué que l'affectation de professionnels expérimentés et de formation universitaire serait sans doute plus appropriée.

Voilà un point qu'il convient malheureusement de répéter. Car, même si les nouveaux recherchistes nommés à ce service ont fait des études universitaires, ils ne possèdent pas la vaste expérience de la recherche et du gouvernement que nous considérons comme essentielle.

De plus, ces recherchistes ne sont que temporairement affectés au service de recherche. Ils sont destinés à être remplacés par des employés qui seront classés à un niveau inférieur et qui auront besoin de formation.

Nous croyons également que le service de recherche pourrait être utilisé à meilleur escient. Les membres de ce service découpent maintenant des articles des médias et recherchent dans les bases de données les informations demandées par les enquêteurs et les analystes.

Les recherchistes ne font pas d'analyses et ne rédigent même pas des résumés des informations contenues dans les dossiers. Il s'agit là d'une occasion ratée. Il est impossible de ne pas se demander si cette façon de procéder reflète l'approche axée sur les cas du travail policier.

Nous pensons comme la Commission McDonald que les rapports «devraient attacher moins d'importance aux cas précis et viser davantage à fournir au gouvernement des appréciations à plus long terme et de portée plus générale en ce qui concerne les dangers menaçant la sécurité du Canada*».

Le personnel du service de recherche, en tant que recherchistes actifs, occupe une place unique pour donner au Service une perspective globale—par exemple pour repérer les nouvelles tendances qui font jour.

La Section de l'information de sources ouvertes a deux façons de traiter l'information. De son Centre des opérations d'urgence, elle peut obtenir rapidement des informations sur les événements rapportés subitement à titre d'actualité par les médias. Elle puise également des informations dans les coupures de presse et les bases de données informatisées.

L'approche est plus globale que par le passé, mais elle soulève toujours la question de savoir si le personnel de recherche pourrait jouer un rôle analytique plus important.

Autres besoins. Nos recherches révèlent que l'utilisation qui est faite de la Section de l'information de sources ouvertes par les services opérationnels n'est pas systématiquement enregistrée ni analysée. Nous croyons que cette mesure devrait précéder toute tentative pour déterminer comment la Section pourrait être consultée plus efficacement.

---

* *La liberté et la sécurité devant la loi*, deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981, p. 640).

Nous encourageons également le Service à compléter son réseau de centres de référence régionaux aussi rapidement que possible.

Centre d'information de la police canadienne

Malgré certaines améliorations apportées en 1986-1987, l'accès du Service au Centre d'information de la police canadienne (CIPC) laisse gravement à désirer.

Le CIPC est un réseau informatique à liaison radio qui donne aux agents de la GRC et des forces policières à l'échelle provinciale et à l'échelle municipale un accès instantané à l'information figurant dans trois banques de données de la GRC. Ces banques donnent :

- l'immatriculation des véhicules;
- les dossiers judiciaires des particuliers et les mandats d'arrêt non exécutés les concernant;
- d'autres informations pertinentes sur ces particuliers.

L'utilité éventuelle du CIPC pour le SCRS est évidente. L'accès immédiat aux informations sur les immatriculations des véhicules serait à lui seul un secours inestimable aux surveillants du SCRS lorsqu'ils filent des cibles.

Mais le Service a dû lutter étape par étape en vue d'obtenir l'accès même partiel dont il jouit.

La raison—boiteuse—qu'on nous a donnée est que le CIPC a été conçu pour desservir les «agents de la paix» et que les enquêteurs du SCRS ne sont pas, techniquement parlant, des «agents de la paix».

Ne coupons pas les cheveux en quatre. Lorsque le CIPC a été mis sur pied, la responsabilité du renseignement de sécurité a été attribuée à la GRC, et les personnes qui s'acquittaient de cette responsabilité étaient des agents de la paix. Au SCRS, ce sont des civils sans, par exemple, les pouvoirs d'arrestation d'un agent de la paix.

Mêmes fonctions. Cependant, les enquêteurs du SCRS ont exactement les mêmes fonctions et responsabilités que les anciens enquêteurs de la GRC chargés du renseignement de sécurité. Le CIPC est aussi nécessaire au renseignement de sécurité aujourd'hui qu'il l'était à l'époque.

Dans nos deux derniers rapports annuels, nous avons exprimé notre frustration à l'égard des difficultés qu'éprouvait le SCRS à accéder directement au CIPC. Nous avons discuté de la question avec le commissaire de la GRC en personne. Enfin, dans notre dernier rapport annuel, nous avons engagé le solliciteur général, qui est responsable à la fois du SCRS et de la GRC, à intervenir.

C'est ce qu'il a fait, et le Comité consultatif du CIPC a depuis lors accordé au SCRS un accès direct à la banque de données sur l'immatriculation des véhicules. Mais l'accès direct aux autres banques se limite aux opérations d'antiterrorisme.

Lorsque le SCRS veut obtenir d'autres informations du CIPC, sur le casier judiciaire d'une cible d'antisubversion, par exemple, il doit se rendre à la GRC, qui interroge le terminal et lui remet l'imprimé.

Cette procédure entraîne des retards inutiles et donne la fausse impression que le SCRS est un simple associé de la GRC.

Conflit de compétences. Même l'accès direct limité dont bénéficie actuellement le SCRS est imparfait—pour ne pas dire plus. À la fin de 1986-1987, la GRC lui avait seulement fourni quatre terminaux du CIPC. Il n'y avait toujours pas de terminal à l'Administration centrale du SCRS. Des terminaux avaient été commandés, mais nous sommes persuadés que les retards sont dus au fait que la GRC ne voulait toujours pas traiter le SCRS sur un pied d'égalité.

Entre-temps, des milliers de policiers dans des banlieues paisibles ont des terminaux du CIPC montés sous les tableaux de bord de leurs voitures et peuvent se renseigner aussi facilement sur des adolescents qui traînent dans un parc de stationnement que sur la voiture dans laquelle les voleurs d'une banque se sont enfuis.

Mais aucun surveillant du SCRS aux trousses d'un présumé terroriste n'a la même possibilité d'obtenir des renseignements instantanés sur sa proie.

Nous ne voyons pas pourquoi le SCRS devrait s'accommoder d'un accès moins qu'illimité et pourquoi il ne pourrait pas être doté d'un nombre suffisant de terminaux. Voilà un exemple classique d'établissements ayant de grandes responsabilités qui donnent plutôt la priorité à de mesquins conflits de compétences.

Les universités et le gouvernement

Des inquiétudes ont été exprimées devant diverses instances, dont le Comité permanent de la Chambre des communes chargé de la justice et du solliciteur général, concernant les interrogatoires faites au hasard à des établissements d'enseignement postsecondaires et l'utilisation des fonctionnaires comme informateurs réguliers.

Établissements d'enseignement postsecondaires. La collecte de l'information aux institutions de haut savoir doit maintenir un équilibre délicat entre deux valeurs sociales.

D'une part, la liberté universitaire suppose l'occasion, et même le devoir, d'exprimer des opinions contraires paisiblement, sans crainte de harcèlement. L'histoire enseigne que l'ordre social d'une génération repose souvent sur le radicalisme de la génération précédente. La démocratie elle-même tombe parfois en discrédit.

D'autre part, le SCRS doit être en mesure de mener ses enquêtes partout où l'amènent les agents de renseignements hostiles ou leurs représentants, les terroristes ou les tenants d'idées subversives.

Nous confirmons que les indications et la politique du solliciteur général concernant les opérations du SCRS aux campus sont conformes à la position établie pour la GRC et approuvée par l'Association canadienne des professeurs d'université en 1963, à savoir :

> Il n'y a actuellement aucune surveillance générale de la GRC aux campus universitaires. La GRC se rend aux universités au besoin, dans le cadre de ses fonctions liées à la sécurité, pour recueillir des informations sur les personnes postulant un emploi dans la Fonction publique ou si elle a des raisons précises de penser que des particuliers exercent de l'espionnage ou se livrent à des activités subversives.

Les activités en question sont maintenant définies à l'article 2 de la *Loi sur le SCRS* comme des «menaces envers la sécurité du Canada».

La décision de s'adonner à des activités d'enquête sur les campus est aussi limitée par une directive ministérielle du 8 juin 1984. Cette directive prévoit qu'il faut faire enquête seulement lorsqu'il existe des raisons objectives de penser que des particuliers se livrent à des activités qui sont préjudiciables au Canada, et elle exige l'approbation ministérielle de certains types d'enquête.

Fonctionnaires en tant que sources. De même, des craintes ont été exprimées concernant l'utilisation des fonctionnaires fédéraux comme sources, parce qu'ils pourraient se sentir tenus de collaborer avec le SCRS pour protéger leur emploi.

Une directive secrète du solliciteur général énonce les principes généraux régissant l'utilisation des employés fédéraux comme sources.

Ententes entre organisations au Canada

Mise à part la question des sources humaines occupant des postes au gouvernement fédéral, le SCRS doit, pour faire son travail efficacement et effectivement, avoir accès aux dossiers des forces policières et d'autres organismes gouvernementaux—aux échelles fédérale, provinciale et locale ainsi qu'à l'étranger.

Le partenaire le plus important du SCRS est probablement la GRC. En fait, les répercussions de leurs relations sont si nombreuses que nous les étudions dans une partie spéciale du chapitre 5.

Les ententes officielles entre le SCRS et d'autres organismes doivent être préalablement approuvées par le solliciteur général, et nous les examinons après coup.

Ministères fédéraux. En 1986-1987, nous avons reçu copie de protocoles d'entente avec trois ministères fédéraux, donnant au SCRS l'accès aux renseignements personnels permis par l'alinéa 8(2)e) de la *Loi sur la protection des renseignements personnels*—à savoir, l'accès à des renseignements nécessaires en vue de faire respecter une loi ou de tenir une enquête licite.

Les ministères sont Revenu Canada (Douanes et Accise), le Secrétariat d'État et la Commission de l'emploi et de l'immigration du Canada. Deux ententes ont été signées avec la Commission.

Ces dernières ont porté à six le nombre total d'ententes avec des ministères et organismes fédéraux; des ententes existaient déjà avec Postes Canada* et le ministère des Affaires extérieures.

Nous sommes convaincus que ces ententes protègent adéquatement la vie privée des particuliers tout en fournissant au SCRS un accès suffisant pour faire son travail.

Provinces et police. En 1986-1987, nous avons reçu copie de cinq protocoles d'entente prévoyant la liaison et l'échange d'informations avec les ministères provinciaux et avec des forces policières autres que la GRC.

Ces ententes ont été conclues avec la Colombie-Britannique, l'Alberta, l'Ontario, l'Île-du-Prince-Edouard et la Nouvelle-Écosse.

Nous les avons trouvées acceptables du point de vue de la sécurité.

Mais nous notons avec une certaine inquiétude qu'elles ne semblent pas obligatoires. Nous espérons qu'elles ne donneront pas lieu à des problèmes si le SCRS a ultérieurement besoin d'informations que les provinces ou la police sont, pour leurs propres raisons, peu disposées à donner.

Nous saisissons également cette occasion pour suggérer que le SCRS tienne des notes complètes et exactes de tous ses contacts en vertu de ces protocoles.

Et nous conseillons vivement la négociation en priorité d'ententes avec les autres provinces afin d'assurer au besoin un flux d'information rapide et régulier dans les deux sens.

Ententes avec l'étranger

Les ententes avec les gouvernements étrangers prévoient généralement des échanges d'information destinés à combler trois besoins—l'examen des demandes de visas et d'immigration, l'octroi des habilitations de sécurité et, enfin, la protection des intérêts nationaux respectifs du Canada et de l'autre pays.

Le SCRS a également pris avec ses agences soeurs de sécurité et de renseignements des arrangements de collaboration dans des secteurs comme le perfectionnement professionnel.

* Plus tôt, nous avons indiqué qu'une entente relative aux opérations d'ouverture du courrier est toujours en voie de négociation avec Postes Canada. L'entente mentionnée ici, concerne les propres dossiers de Postes Canada.

En 1986-1987, nous avons reçu copie de cinq ententes nouvelles et révisées intervenues avec des gouvernements étrangers. Nous avons également vu des exemplaires de l'instruction ministérielle autorisant chaque entente. Toutes étaient en règle.

On craignait que le SCRS ne fasse pas clairement la différence entre les ententes de liaison avec l'étranger qui étaient simplement souhaitables et celles qui étaient strictement nécessaires.

Nous sommes d'avis, et les opinions juridiques indépendantes que nous avons reçues le confirment, que la règle du «strictement nécessaire» énoncée dans la *Loi sur le SCRS* (article 12) ne s'applique pas à la signature d'ententes avec les gouvernements étrangers. Il suffit que de telles ententes favorisent la protection de la sécurité nationale. Néanmoins, nous sommes heureux que le solliciteur général ait demandé au SCRS de faire plus clairement état de ses besoins dans ses propositions visant de nouvelles ententes.

Afin que, dorénavant, nous soyons davantage en mesure de réviser les ententes avec les gouvernements étrangers, nous avons demandé au solliciteur général de commencer à nous envoyer des exemplaires des lettres dans lesquelles le secrétaire d'État aux Affaires extérieures commente chaque arrangement qui est proposé.

Deux questions qui se posent toujours en ce qui concerne la liaison avec l'étranger exigent des observations particulières— d'abord, «l'héritage» des arrangements négociés par la GRC et, ensuite, la position des agents de liaison du SCRS dans certaines missions canadiennes à l'étranger.

L'héritage de la GRC. Au début de 1985, nous avons reçu du SCRS des milliers de pages dont il avait hérité de l'ancien service de sécurité de la GRC, lesquelles exposaient les arrangements existants avec des gouvernements étrangers et leurs agences. Dans nos derniers rapports annuels, nous recommandions que ces arrangements soient revus à la lumière de la nouvelle *Loi sur le SCRS* et renégociés.

Depuis lors, une nouvelle refonte des arrangements avec l'étranger a été préparée, examinée par le ministère des Affaires extérieures et approuvée par le solliciteur général.

Nous en sommes arrivés à la conclusion, appuyée par des opinions juridiques indépendantes, que les dispositions sur la transition de la *Loi sur le SCRS* sont suffisamment vastes pour valider les arrangements préalablement conclus par la GRC avec des organismes étrangers. La renégociation serait donc inutile pour des motifs purement juridiques.

Pendant la refonte, le SCRS a aussi laissé certains arrangements venir à échéance. Cette décision était sensée; certains arrangements qui convenaient à une force policière comme la GRC (dont les membres ont, par exemple, des pouvoirs d'arrestation) ne convenaient pas à un service civil de sécurité et de renseignements (dont les membres n'ont pas les mêmes pouvoirs).

Agents de liaison. Le SCRS a des agents de liaison — sécurité dans des missions canadiennes à l'étranger, lesquels sont chargés de fournir au Service et aux autorités des pays

d'accueil des renseignements opportuns et pertinents et des évaluations sur des questions touchant à la sécurité.

Nous avons examiné le rôle de ces agents et le jugeons conforme à la *Loi sur le SCRS*.

Cependant, nous avons remarqué une certaine confusion en ce qui concerne les responsabilités qui incombent respectivement aux agents de liaison du SCRS et à ceux de la GRC qui sont également affectés à certaines missions. Nous reviendrons à ce sujet dans nos commentaires généraux sur les relations SCRS-GRC (page 34).

Actes illégaux

Le directeur a déclaré, conformément à la *Loi sur le SCRS* (article 20), qu'un employé peut avoir enfreint la loi dans l'exercice de ses fonctions en négligeant, à deux différentes reprises, d'obtenir la signature d'usage d'un superviseur sur des documents autorisant certains actes. L'employé a été réprimandé et est maintenant parfaitement conscient de cette exigence. Nous convenons qu'il n'y a pas lieu de porter des accusations.

Il y a également eu quelques incidents où la direction du SCRS a enquêté sur des écarts de conduite commis par des employés en dehors des heures de travail. Ces enquêtes ont entraîné la démission ou le renvoi des personnes concernées. Comme elles ne sont pas liées au travail du Service, nous les considérons comme des questions d'administration du personnel.

Relations privilégiées entre un avocat et ses clients. Cependant, il y a eu une faute grave que le directeur n'a pas signalée. Des documents portant sur des communications entre un avocat et ses clients ont été retenus dans trois des cinq régions du Service pendant environ un an, ce qui allait à l'encontre des conditions imposées par les juges de la Cour fédérale dans les mandats concernés.

Le problème découlait d'une interprétation fausse des nouvelles instructions de l'Administration centrale concernant la conservation des dossiers en général. Il a rapidement été corrigé lorsqu'il a été découvert. À cause de leur nature privilégiée, les documents ont été scellés et sont tous en voie de destruction, comme les mandats l'exigeaient.

Une lacune. À court terme, aucun dommage matériel n'a été causé. Nous avons lu le rapport de l'inspecteur général qui, après une enquête poussée, en est arrivé à la même conclusion. Cependant, cette situation fait ressortir une lacune de la *Loi sur le SCRS* : contrairement au *Code criminel*, elle n'offre aucune protection aux communications entre un avocat et ses clients.

À première vue, cela est inquiétant. Les gens devraient être libres de discuter de leurs affaires juridiques en toute franchise avec leur avocat, sans craindre que leurs paroles ne soient divulguées sans leur consentement. C'est là l'essence du privilège avocat-client.

Nous avons donc examiné cette question de près et nous l'avons discutée à trois différentes reprises avec les sous-directeurs du SCRS.

Par suite de rapports dans les médias*, nous avons aussi enquêté sur un cas particulier où les communications entre un avocat et son client avaient été interceptées. Nous sommes convaincus que, dans cette affaire, l'interception était justifiée pour des motifs de sécurité valables. Nous avons également noté que l'information acquise n'a été transmise à aucun autre organisme.

Équilibre délicat. Il nous restait donc à étudier la question globale. Comme dans tant d'autres secteurs du renseignement de sécurité, un équilibre délicat doit être maintenu.

En faisant abstraction de tout incident particulier, nous pouvons facilement imaginer des circonstances où l'interception des communications serait justifiée—par exemple lorsqu'un avocat semble avoir conspiré contre l'intérêt national avec le «client» ou lorsqu'il transmet des messages pour les conspirateurs. Même le *Code criminel* n'est pas assez large pour protéger des communications qui concernent des actes illégaux impliquant l'avocat.

Les juges de la Cour fédérale ont pour pratique d'inclure dans les mandats judiciaires des protections particulières visant les communications privilégiées entre un avocat et ses clients. Ainsi, ils peuvent :

- Interdire l'interception de communications au bureau ou au domicile d'un avocat ou à tout autre endroit où un avocat consulte normalement ses clients. (Le *Code criminel* offre la même protection.)
- Restreindre l'interception des appels entre la cible et l'avocat (ou l'employé de l'avocat) aux appels qui, selon le directeur ou un directeur général de région, sont liés à la menace qui est précisée dans le mandat judiciaire.

Arrangements actuels. Le SCRS a des procédures spéciales pour remplir ces conditions. Tout document concernant des communications entre un avocat et le client est soumis au directeur ou à un directeur général de région. S'il détermine que la communication ne constitue pas une menace envers la sécurité du Canada, tous les documents concernant la communication sont détruits et aucune autre divulgation n'est faite.

Sauf dans les cas décrits précédemment, nous croyons que ces procédures sont suivies. Mais nous ne sommes pas convaincus qu'elles soient suffisantes.

Nous craignons notamment que, à l'instar de l'examen des demandes de mandats judiciaires par le solliciteur général et notre examen des dossiers opérationnels sur lesquels elles s'appuient, ces mesures protectrices soient fondées sur l'engagement personnel— celui des juges de la Cour fédérale à continuer de les inscrire dans les mandats judiciaires. Si elles ne deviennent pas loi, cette pratique pourrait changer n'importe quand.

Le Parlement pourrait aussi vouloir étudier cette question au moment de l'examen quinquennal de la *Loi sur le SCRS*.

---

* Notamment dans *The Globe and Mail*, Toronto, 8 janvier 1987.

4. Ce que sait le SCRS

Ayant examiné dans le dernier chapitre comment le SCRS recueille ses informations, nous passons maintenant à la façon dont il les gère. Le SCRS conserve-t-il des informations confidentielles dont il n'a pas besoin, surtout au sujet de particuliers canadiens? Comment se sert-il des informations qu'il accumule? Dans le présent chapitre, nous nous penchons sur la première question, et nous traiterons de la deuxième au chapitre 5.

Limites légales

La *Loi sur le SCRS* apporte deux limites importantes à la collecte de l'information, à savoir :

- L'information doit être liée aux «menaces envers la sécurité du Canada» (article 2).
- Il ne faut recueillir que l'information qui est «strictement nécessaire» pour s'occuper d'activités qui peuvent être raisonnablement considérées comme des menaces (article 12).

Pour des raisons de commodité, il conviendrait peut-être de citer en entier la définition donnée à l'article 2. Elle dit que les «menaces envers la sécurité du Canada» comprennent :

> *a*) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;
>
> *b*) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;
>
> *c*) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger;
>
> *d*) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence.
>
> La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas *a*) à *d*).

Information héritée

Ce sujet soulève de graves questions d'ordre juridique aussi bien qu'éthique concernant l'information contenue dans les dossiers opérationnels dont le SCRS a hérité du service de sécurité de la GRC.

Une partie de cette information a été recueillie pendant la période troublée décrite par les commissions McDonald et Keable où certains enquêteurs ont laissé leurs authentiques craintes pour la sécurité nationale l'emporter sur leur souci de la vie privée et de la liberté d'opinion exprimée démocratiquement. Nous songeons aussi à l'information remontant à la période du triomphe de la contestation et de la Nouvelle gauche, comme on l'a nommée, dans les années 1960.

Personne ne sait tout ce que ces dossiers contiennent parce qu'ils n'ont pas tous été systématiquement examinés. Mais, vu les constatations des commissions McDonald et Keable, on est justifié de poser les questions suivantes : Cette information correspond-elle toute à la définition d'une menace envers la sécurité du Canada prévue à l'article 2? Est-elle encore toute strictement nécessaire, comme l'exige l'article 12?

Si la réponse à l'une ou l'autre de ces questions est négative, alors d'autres questions se posent : Le SCRS a-t-il le pouvoir légal de garder des renseignements inutiles ou non pertinents dans ses dossiers? Pourrait-on contester devant les tribunaux des initiatives fondées sur ces renseignements?

Le SCRS a résisté à nos pressions pour qu'il examine tous ces dossiers et supprime les éléments qui ne répondent pas aux exigences des articles 2 et 12. Il existe, nous l'admettons, des difficultés réelles.

Moratoire. À court terme, il y a le moratoire sur la destruction des dossiers décrété après que la Commission Deschênes eut découvert que des vieux dossiers d'immigration dont elle avait besoin pour son enquête sur d'allégués criminels de guerre avaient été couramment détruits. Nous revenons à la question des dossiers périmés du SCRS dans un instant.

Même si le moratoire était levé, dépouiller ces dossiers un à un et radier toutes les informations qu'ils ne devraient pas renfermer serait une tâche gargantuesque.

D'autre part, nous devons reconnaître que le travail du SCRS consiste justement à rechercher et à déceler des menaces éventuelles dans des bribes d'information apparemment innocentes.

De toute façon, d'après le SCRS, il devrait suffire que les renseignements qui ne devraient pas figurer dans ces dossiers ne soient pas utilisés; c'est là d'ailleurs le rôle de notre Comité—de sonner l'alarme si des limites comme la règle du «strictement nécessaire» sont outrepassées.

Nous ne voulons pas esquiver notre responsabilité consistant à contrôler l'utilisation de l'information par le Service. Mais nous avons un problème de taille : nous ne pouvons pas vraiment soumettre chaque membre du Service à une surveillance de tous les instants. Et nous avons du mal à imaginer que des renseignements non pertinents, même s'ils ne sont pas techniquement «utilisés», n'influenceraient pas tant soit peu l'enquêteur ou l'analyste qui en prendrait connaissance.

Ainsi, nous aimerions encore voir ces dossiers systématiquement épurés. Cette tâche pourrait être ramenée à des proportions raisonnables si elle s'étalait sur plusieurs années et faisait l'objet d'un échéancier précis.

Nous avons été heureux d'apprendre pendant l'année que le solliciteur général partage nos préoccupations et qu'il a demandé au SCRS d'élaborer, conformément aux articles 2 et 12 de la *Loi sur ie SCRS*, des normes visant les informations à conserver dans les dossiers.

Fermeture des vieux dossiers

Cela nous ramène à la question posée par la fermeture et la destruction de dossiers complets qui ne sont plus utiles—préoccupation dont nous avons hérité de la Commission McDonald*.

Par suite des observations de la Commission McDonald, le service de sécurité de la GRC et l'archiviste fédéral—qui est chargé d'évaluer et d'approuver les propositions en vue de conserver ou de détruire les dossiers fédéraux—ont établi des échéanciers pour la destruction des dossiers inactifs.

À la fin des années 1970, il y a eu une destruction massive de dossiers qui avaient été ouverts avant 1973. Ensuite, entre juillet 1984, mois où le SCRS a pris la succession du service de sécurité, et février 1985, celui où le moratoire susmentionné a pris effet, quelque 77 800 dossiers sans valeur pour le renseignement de sécurité ont été détruits après examen.

Aujourd'hui, plus de 67 000 dossiers sont prêts à être détruits à la fin du moratoire.

Nous avons l'oeil sur cette question et avons demandé des exemplaires des échéanciers de destruction. Nous notons que la politique du gouvernement prévoit l'examen quinquennal de ces échéanciers, et nous avons été encouragés d'apprendre que le SCRS a amorcé un tel examen avec l'archiviste fédéral en décembre 1986.

Renseignements étrangers

Une autre question est ressortie de notre examen du flux d'information dans une direction opérationnelle du SCRS.

Il nous semblait que le SCRS avait peut-être trop tendance à accepter d'emblée l'information fournie par les services de renseignements de pays amis; il ne l'examine peut-être pas d'un oeil aussi critique que l'information émanant de sources canadiennes.

À vrai dire, il nous semblait que le SCRS était peut-être trop prêt à accepter la politique étrangère sous-tendant cette information plutôt qu'à l'adapter à la politique canadienne (voir, par exemple, la page 41 du présent rapport). Le Canada a ses propres intérêts nationaux, qui diffèrent de ceux de toute autre nation.

La Commission McDonald a signalé qu'il était dangereux «d'épouser les façons de voir et les opinions d'un service étranger, particulièrement d'un organe dont il [le service canadien] vient à dépendre dans une large mesure**». Cette mise en garde reste valable.

---

* *La liberté et la sécurité devant la loi*, deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981), p. 547.

** *La liberté et la sécurité devant la loi*, deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981), p. 666.

Le poids qui est dû. La *Loi sur le SCRS* exige que le Service consulte le ministère des Affaires extérieures sur divers aspects des relations internationales (alinéas 17(1)b) et 19(2)b)). Nous encourageons le SCRS et ce ministère à collaborer plus étroitement à l'évaluation des événements internationaux et à la conduite des activités du SCRS de façon à s'assurer que la politique étrangère du Canada reçoit le poids qui lui est dû.

La Commission McDonald a aussi noté, incidemment, que l'utilisation accrue de l'information de sources ouvertes constituerait un rempart contre un recours excessif aux agences étrangères. Cette observation vient appuyer notre allégation que le SCRS devrait faire davantage appel aux sources ouvertes (voir la page 15 du présent rapport).

Information indirecte

En 1986, le SCRS a élaboré une nouvelle politique pour traiter l'information qu'il acquiert par inadvertance mais qui n'a rien à voir avec la sécurité nationale. Il répartit cette information en deux catégories : celle qui est utile et celle qui ne l'est pas.

L'information de la première catégorie pourrait éventuellement servir à l'application de la législation criminelle, à la défense nationale, à la conduite des relations extérieures ou à la poursuite générale de l'intérêt national. Nous l'examinons dans le prochain chapitre.

La deuxième catégorie contient toutes les informations qui ne sont pas nécessaires à la sécurité nationale. Elle sont, à juste titre, détruites.

Il y a des types d'informations auxquelles le SCRS devrait clairement être sourd—et muet. Par exemple, il ne doit jamais intervenir dans le processus démocratique en communiquant au governement des informations sur la stratégie électorale d'un parti légitime de l'opposition. Nous croyons qu'il ne l'a jamais fait.

5. Ce que fait le SCRS

Le facteur décisif est l'utilisation qui est faite de l'information du SCRS. Certaines questions qui en découlent font l'objet du présent chapitre. La collaboration avec la police étant l'une des grandes utilisations qui peuvent être faites de l'information du SCRS, les relations opérationnelles avec la GRC sont également traitées ici.

Information indirecte qui pourrait être utile

Nous avons terminé le dernier chapitre par une discussion sur «l'information indirecte» qui est détruite parce qu'elle n'est pas utile pour la sécurité nationale, pour l'application de la législation criminelle, pour la défense nationale, pour la conduite des relations internationales ni pour l'intérêt national.

L'information qui n'a pas été demandée mais qui pourrait être utile pour l'une de ces fins non liées à la sécurité peut être transmise aux autorités compétentes en vertu de la *Loi sur le SCRS* (article 19).

Si le SCRS diffusait des bulletins contenant cette information à tout-venant, nous pourrions croire qu'il tend un filet plus large que «strictement nécessaire» (article 12 de la *Loi sur le SCRS*) et qu'il s'intéresse à plus qu'à des menaces envers la sécurité du Canada.

En fait, nous craignons plutôt que le Service ne semble trop prudent à cet égard.

Le SCRS en cour

Le public a pu se rendre compte à plusieurs reprises combien le Service est jaloux de ses secrets, lorsque ses agents ont interrompu des procès et les interrogatoires de leurs collègues en citant la *Loi sur la preuve au Canada*. Le paragraphe 36.1(1) de cette *Loi* dit ceci :

> Un ministre de la Couronne du chef du Canada ou toute autre personne intéressée peut s'opposer à la divulgation de renseignements devant un tribunal, un organisme ou une personne ayant le pouvoir de contraindre à la production de renseignements, en attestant verbalement ou par écrit devant eux que ces renseignements ne devraient pas être divulgués pour des raisons d'intérêt public déterminées.

L'article 36.2 prévoit que les oppositions peuvent être entendues par la Cour fédérale du Canada lorsqu'il est allégué que la divulgation «porterait préjudice aux relations internationales ou à la défense ou à la sécurité». Il permet aussi les appels.

Des manchettes comme «Spywork : How can it close down a court» (*Toronto Star*, 21 juin 1986) et «Gag order needs no reasons» (*Ottawa Citizen*, 7 juin 1986) ont résulté des interventions du SCRS en vertu de la *Loi sur la preuve au Canada*.

Cela n'a rien de surprenant. Tous les services de sécurité et de renseignements cherchent à cacher leurs sources et à garder les secrets du «métier». La protection des sources humaines constitue une préoccupation spéciale. Un informateur qui perd son identité d'emprunt risque de ne plus être utile. Et les sources éventuelles tourneront sûrement le dos à un service qui ne les protège pas contre la notoriété publique et ses conséquences.

Toutes les preuves pertinentes. Néanmoins, nous estimons qu'il devrait y avoir des façons de garantir que les tribunaux—à défaut du public—entendent toutes les preuves pertinentes dans les causes criminelles. D'abord, les preuves du SCRS pourraient même tendre à prouver l'innocence de l'accusé; dans pareil cas, le silence semble affaiblir le principe fondamental que, devant nos tribunaux, une personne est innocente jusqu'à ce qu'elle soit prouvée coupable.

Nous notons que le *Code criminel*, à l'article 442, prévoit que le public peut être exclu de la salle d'audience lorsque cela est dans l'intérêt «de la moralité publique, du maintien de l'ordre ou de la bonne administration de la justice».

Doit-on ajouter la «sécurité nationale» à la liste? Le problème est que l'accusé, qui pourrait être fort intéressé par l'identité des informateurs et les procédures du SCRS, ne serait pas exclu.

Il n'y a donc pas de réponse facile. Il s'agit là d'une autre question que le Parlement pourrait vouloir soulever au moment de l'examen quinquennal de la *Loi sur le SCRS* en 1989.

Aide à la police

Cela nous amène à la question des relations du SCRS avec la police. Car la cour n'est pas le seul endroit où le SCRS ne desserre pas les lèvres. Son désir de garder ses opérations secrètes semble à l'occasion l'avoir porté à cacher des informations à la police.

Nous pensons comme la Commission McDonald* que le SCRS est normalement tenu de transmettre à la police ses informations concernant des activités criminelles. Si, par exemple, un surveillant stationné à l'ombre voit quelqu'un tailler furtivement dans la vitrine d'une bijouterie, ressemblant pour tout au monde à un cambrioleur au travail, la police doit normalement être prévenue. Cela est permis en vertu de l'alinéa 19(2)a) de la *Loi sur le SCRS*.

Nous admettons qu'il y a des exceptions—lorsqu'une enquête policière, et peut-être des preuves produites à un procès subséquent, compromettraient irrémédiablement une opération de sécurité vitale. Par exemple, si l'arrivée d'une voiture de police pousserait des cibles importantes à se rendre à un nouvel emplacement inconnu du Service.

Les directeurs généraux des régions décident si les informations concernant les activités criminelles doivent être transmises à la police. Les lignes directrices sont exposées dans un bulletin opérationnel publié sous l'autorité du directeur du SCRS.

Le bien-fondé. Les règles prévoient essentiellement que le bien-fondé de chaque affaire est étudié d'après la gravité du délit supposé, la protection des sources du SCRS et la possibilité de nuire à la capacité opérationnelle du SCRS si l'on apprend qu'il a aidé à dévoiler le délit. Le Service étudie le besoin de lignes directrices plus formelles.

---

* *La liberté et la sécurité devant la loi*, deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981), page 637.

Notre préférence est déjà claire. Nous sommes heureux de voir les directeurs généraux des régions prendre des décisions. Mais nous croyons que les critères devraient être énoncés dans une nouvelle directive ministérielle, afin de les protéger contre tout changement arbitraire que le SCRS pourrait lui-même apporter à l'avenir.

Relations avec la GRC

Les gestionnaires supérieurs du SCRS et de la GRC semblent de plus en plus satisfaits de la ligne de démarcation entre leurs responsabilités respectives, mais il a manifestement été plus difficile de tracer cette ligne petit à petit sur le terrain.

Le terme «saine tension» a été utilisé pour décrire la situation, mais nous croyons qu'un peu moins de tension serait encore plus sain. Nous sommes toutefois encouragés par le fait que l'on reconnaît les problèmes et que l'on prend des mesures pour y remédier.

Le solliciteur général nous a remis un exemplaire d'un protocole d'entente entre la GRC et le SCRS, où est réuni un certain nombre d'arrangements visant la collaboration et le partage des services et de l'administration.

Il nous a informés qu'il avait reporté l'approbation des chapitres sur le CIPC et le partage de l'information. Nous appuyons sa décision. Nous avons déjà discuté du CIPC (page 17 du présent rapport). Quant au partage de l'information, nous avons écrit au solliciteur général pour l'avertir que les efforts du SCRS et de la Direction de renseignements criminels de la GRC pourraient faire double emploi.

Sauf ces réserves, le protocole d'entente jette des bases solides pour des relations qui sont plus harmonieuses parce qu'elles sont clairement définies dans un certain nombre de domaines aussi prosaïques que le logement, les services aériens, les services de traduction multilingue, l'administration des traitements, les services photographiques, l'impression et l'utilisation d'appareils sûrs pour les télécommunications et le traitement électronique des données.

Agents de liaison. Le solliciteur général a établi un échange d'agents de liaison dans les programmes d'antiterrorisme du SCRS et de la GRC pendant le deuxième semestre de 1986.

C'est dans le domaine de l'antiterrorisme que les mandats du SCRS et de la GRC se recoupent le plus étroitement et c'est là aussi qu'ils sont le plus susceptibles d'accrocher. Il y a, comme le directeur du SCRS entre autres l'a signalé*, deux besoins dans ce secteur.

Primo, des renseignements sont requis pour prédire et empêcher les incidents—ce besoin est la responsabilité du SCRS. Secundo, les criminels doivent être appréhendés et des preuves suffisantes doivent être recueillies pour les condamner—ce besoin fait partie des responsabilités de la GRC en matière d'application de la loi.

---

* Chambre des communes, *Procès-verbaux et témoignages du Comité permanent de la justice et du solliciteur général*, 11 décembre 1986.

Lorsqu'il y a conspiration criminelle et avant qu'un incident se produise, les deux domaines se chevauchent. La collaboration entre le SCRS et la GRC est manifestement essentielle. La *Loi sur le SCRS* prévoit ce chevauchement en énumérant clairement les responsabilités respectives du SCRS et de la GRC en matière de renseignements et d'application de la loi (articles 12 et 61).

Alerte à l'aéroport

Malheureusement, en étudiant une opération d'antiterrorisme—«l'alerte à l'aéroport»—nous avons découvert des conflits de compétences et de la méfiance.

L'incident a commencé en décembre 1985, mois où la police a été informée d'un présumé complot libyen visant à placer une bombe à bord d'un aéronef commercial en partance d'Ottawa.

Les mesures de sécurité ont subséquemment été renforcées aux principaux aéroports, ce qui a coûté fort cher aux contribuables canadiens et a considérablement dérangé—pour ne pas dire inquiété—les voyageurs. En outre, la menace a empêché le personnel affecté à la sécurité publique de remplir d'autres fonctions importantes et elle a perturbé les enquêtes policières courantes.

Soit parce que l'information était frivole ou parce que le complot a été rapidement dévoilé et que les efforts en vue d'y faire obstacle ont entraîné son annulation, il n'y a pas eu d'explosion. La sécurité aux aéroports est redevenue normale.

Étude de cas. Les Canadiens, qui avaient encore frais à l'esprit les désastres d'Air India et de l'aéroport Narita en 1985, ont poussé un soupir de soulagement et sont retournés à leurs occupations normales. Nous avons fait de même et saisi l'occasion d'étudier à fond comment le SCRS et les forces policières travaillent ensemble dans une opération antiterroriste.

L'incident était un bon exemple d'une affaire où l'antiterrorisme, les enquêtes criminelles et le renseignement de sécurité s'imbriquent, exigeant la collaboration étroite des divers intervenants dans le cadre de leurs rôles et fonctions.

Nous ne sommes évidemment pas libres de publier la totalité de notre rapport. Outre les raisons de sécurité, nous avons promis un traitement confidentiel à certains de nos informateurs en échange de leur collaboration. La GRC et la Police d'Ottawa, qui étaient responsables de l'enquête au criminel, ne nous rendent pas compte. Mais nous les remercions, ainsi que le SCRS, de leur aide constante sans faille pendant cette enquête.

Cependant, nous avons présenté au solliciteur général un rapport qui contenait nos conclusions et recommandations.

Réticence. Il n'était pas clair selon nous que le SCRS était membre à part entière du groupe de travail spécial qui a été formé pour traquer les présumés conspirateurs. Il est

vite devenu très évident que le flux d'information entre le SCRS et la police aurait pu être meilleur.

Cette réticence était à double sens. La police, qui a été prévenue la première, a attendu six jours avant d'appeler le SCRS à son aide, par exemple. Nous avions l'impression que la GRC, en particulier, estimait que l'opération était exclusivement policière.

D'autre part, le SCRS a manqué une occasion de dissiper cette impression en déclinant une invitation de participer à une surveillance.

Lignes directrices. À vrai dire, nous avons découvert que le SCRS et la GRC n'avaient pas encore complètement fait accorder leur mandat respectif dans le domaine de l'antiterrorisme. L'échange susmentionné d'agents de liaison est un grand pas en avant, mais nous croyons que des procédures opérationnelles plus formelles s'imposent. Il faudrait entre autre traiter des questions suivantes :

- Quelles limites peuvent être apportées à l'utilisation de l'information partagée.
- Comment la responsabilité des fonctions de surveillance doit être partagée.

Entre-temps, nous avons recommandé au ministère du Solliciteur général de contrôler soigneusement l'arrangement de liaison et de tenir le solliciteur général informé des progrès.

Nous avons également recommandé une instruction ministérielle qui encouragerait le partage approprié de l'information dans les enquêtes sur les activités terroristes exigeant l'attention du SCRS et de la GRC, même en ce qui concerne des questions aussi délicates que l'identité des sources, en reconnaissant que les renseignements ultimement requis pour les procédures judiciaires devraient être fournis d'une façon qui protège les futures initiatives dans le secteur du renseignement.

Relations publiques. Nous avons conclu que les forces policières locales ne semblent pas entièrement connaître le rôle du SCRS. Nous avons donc recommandé au SCRS de lancer une campagne de relations publiques qui fournirait aux organismes policiers des informations sur son mandat, son rôle ainsi que ses activités et leur rappellerait qu'il s'agit d'un organisme différent de la GRC.

Cela encouragerait les forces policières locales à traiter directement avec le SRCS aussi bien qu'avec la GRC pour contrer les menaces terroristes.

Dans le même ordre d'idées, nous avons recommandé que le réseau d'ententes de collaboration mutuelle entre le SCRS et les provinces soit complété en priorité (voir la page 20). Aucune entente n'était en vigueur au moment de l'alerte à l'aéroport.

Une protection à toute épreuve ne peut être accordée en tout temps aux aéroports; il y aura toujours des façons de troubler la paix dont jouissent généralement les voyageurs au Canada. C'est pourquoi il est doublement important d'assurer une collaboration sans réserve du type que le solliciteur général cherche à établir entre la GRC et le Service.

Agents de liaison avec l'étranger

Il y a du progrès à l'extérieur du pays, aux missions canadiennes où le SCRS et la GRC ont tous deux des agents de liaison. Il a été convenu que le SCRS examinerait dorénavant les demandes de visa. Nous croyons que cela est conforme à la lettre et à l'esprit de l'article 14 de la *Loi sur le SCRS*.

Notons que le SCRS et la GRC ont des arrangements d'aide mutuelle dans les postes où seulement l'un ou l'autre a un agent de liaison. Cette mesure semble bien marcher.

Persona non grata

Le SCRS a bien utilisé ses conclusions pour déterminer les agents étrangers qui bénéficiaient de l'immunité diplomatique au Canada.

Par suite des informations qu'il a transmises au ministère des Affaires extérieures, deux membres de missions étrangères ont été déclarés *persona non grata* en 1986-1987 et rapatriés. Six autres ont été volontairement rappelés.

L'intérêt public

Des règles légales régissent la divulgation à un ministre autre que le solliciteur général ou, dans des circonstances précises, au secrétaire d'État aux Affaires extérieures, au ministre de la Défense nationale ou à un fonctionnaire d'information qui, aux termes de l'alinéa 19(2)d) de la *Loi sur le SCRS*, est «essentielle pour des raisons d'intérêt public et que celle-ci justifie nettement une éventuelle violation de la vie privée».

Le consentement du solliciteur général est requis et, en vertu du paragraphe 19(3), le directeur doit nous faire rapport par la suite.

Nous n'avons reçu aucun rapport sur la divulgation de tels renseignements en 1986-1987.

Organismes de façade

La *Loi sur le SCRS* n'envisage pas la divulgation d'information à des organismes volontaires ou à leurs membres en cas d'infiltration par des personnes qui peuvent vouloir s'en servir pour des fins qui pourraient représenter une menace envers la sécurité du Canada.

Nous avons soulevé cette question dans notre rapport de l'an passé, signalant que les Canadiens loyaux qui appartiennent à des groupes infiltrés ou menacés d'infiltration méritent d'être alertés si des moyens peuvent être trouvés pour ce faire.

De quelle façon, avons-nous demandé, pourrait-on avertir les personnes qui se joignent à un «organisme de façade»* parce qu'elles appuient ses objectifs officiels que cet organisme a aussi des objectifs cachés?

Nous avons appris depuis lors, pendant des séances d'information du SCRS, que les services de renseignements de pays hostiles avaient, en fait, infiltré certains organismes et qu'un financement considérable de sources étrangères avait été décelé.

Si le SCRS devait publier pareilles informations, il révélerait du même coup des sources d'information soigneusement gardées. Il serait naïf d'affirmer que ceux qui sont surveillés ne le savent pas. Mais la publication de tout détail pourrait compromettre la surveillance.

Nous n'avons pas de réponse facile à offrir. Nous ne faisons que répéter ce que nous avons dit l'an dernier, soit que le Parlement pourra vouloir traiter ce sujet lorsqu'il examinera la *Loi sur le SCRS*.

Un Canadien vigilant. Entre-temps, nous avons été encouragés par un résultat de nos observations à cet égard l'an dernier.

Après avoir lu le passage pertinent de notre rapport annuel, une personne profondément engagée envers une cause a entrepris de poser des questions énergiques et perspicaces au conseil d'administration d'un organisme de façade. Celui-ci a fini par avouer tacitement l'objectif réel de l'organisme, qui n'avait pas grand chose à voir avec cette cause.

Notre lecteur a promptement retiré son appui et il a persuadé d'autres personnes qui pensaient comme lui de lui emboîter le pas.

Si tous les Canadiens étaient aussi vigilants, nous pourrions abandonner nos recherches en vue de trouver une façon de prévenir les membres d'organismes de façade et d'organismes susceptibles d'être infiltrés.

* Voici une définition que nous avons proposée :
«organisme en apparence indépendant dont la promotion d'idées humanitaires, apolitiques et non partisanes sert à cacher d'autres objectifs d'appui à des politiques et objectifs de l'organisme ou de la puissance étrangère qui le contrôle. On ne devrait pas présumer, avons-nous ajouté, que les membres d'un tel organisme connaissent les objectifs cachés, sont d'accord avec ceux-ci ou les appuient».

6. Opérations d'antisubversion

L'utilité du contre-espionnage et de l'antiterrorisme est incontestable. Une nation étrangère donnée nous espionne ou elle ne nous espionne pas. Nous ne pouvons nous opposer au contre-espionnage destiné à protéger nos secrets contre celles qui le font.

De même, il n'y a pas de place pour le terrorisme dans un pays comme le nôtre qui possède des moyens démocratiques bien établis pour acquérir et excercer le pouvoir. Nous pourrions tous être la victime innocente d'un acte terroriste. Clairement, ceux qui veulent se servir de la violence pour atteindre leurs fins politiques doivent être découverts et arrêtés.

L'antisubversion est différente. Le droit de différer paisiblement d'opinion est le fondement de la démocratie. Pourtant, il y a quelques Canadiens qui proclament leur croyance en la révolution violente. Et même l'expression paisible d'opinions différentes peut être secrètement pervertie par des puissances étrangères qui n'ont pas les mêmes objectifs que la plupart des Canadiens.

Zone d'ombre. À quel point un particulier ou un organisme qui exprime une opinion différente devient-il une cible légitime de la Direction de l'antisubversion du SCRS? Quand le bavardage au sujet de la violence devient-il une menace réelle d'actes violents? Quand le contact avec des puissances étrangères devient-il préjudiciable aux intérêts du Canada?

Bien des questions semblables peuvent être posées, et les réponses constituent un terrain propice au dissentiment. C'est pourquoi nous avons fait de l'antisubversion l'objet de notre première étude touchant l'ensemble d'une direction du SCRS.

Nous sommes évidemment limités dans ce que nous pouvons dire. Cependant, nous pouvons décrire notre recherche et présenter certaines conclusions et recommandations.

Soulignons que nos critiques du système ne s'adressent pas aux hommes et aux femmes qui mettent en oeuvre les programmes d'antisubversion. Nous avons été frappés par le dévouement et le talent que la direction et le personnel apportent tous deux à leur travail et par les difficultés réelles que pose l'application de la *Loi sur le SCRS* dans cette zone d'ombre.

Néanmoins, nous avons le devoir d'exprimer les inquiétudes que notre étude nous a suscitées et d'encourager le SCRS à corriger les faiblesses du système.

Les principes et la loi

Pour établir notre norme, nous avons adopté cinq principes fondamentaux de la Commission McDonald*. Les voici :

- La «suprématie du droit» doit être respectée.
- Le moyen d'enquête utilisé doit être proportionnel à la gravité de la menace et à la probabilité de sa mise à exécution.

---

* *La liberté et la sécurité devant la Loi*, deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981), pages 539-540.

- Le besoin d'employer diverses techniques d'enquête doit être mis en regard du tort que cela pourrait causer aux libertés civiles ou à des institutions sociales précieuses.
- Plus une technique comporte d'intrusion, plus l'autorisation d'y recourir doit venir de haut.
- Sauf dans les cas d'urgence, il faut utiliser les techniques de collecte de renseignements qui comportent le moins d'intrusion avant d'employer celles qui en comportent le plus.

Évidemment, nous nous sommes également fondés sur la *Loi sur le SCRS*, notamment :

- La définition de «menaces envers la sécurité du Canada» (article 2), de laquelle le Parlement a veillé à exclure «les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord». (Le texte de la définition figure à la page 25 du présent rapport.)
- L'exigence (article 12) que l'information soit recueillie seulement «dans la mesure strictement nécessaire».

Notre façon de procéder

Dans notre étude, nous avons examiné les procédures directrices et opérationelles afin de déterminer si elles remplissaient les exigences légales, et nous en avons discuté avec la haute direction du SCRS.

Nous avons étudié les processus liés à la planification et à l'obligation de rendre compte, les ressources et les outils d'enquête utilisés dans le secteur de l'antisubversion (comparativement aux ressources et aux outils utilisés par les directions du contre-espionnage et de l'antiterrorisme), le nombre de sources rémunérées, les sommes qui leur sont versées, les procédures de ciblage, le nombre de dossiers ouverts sur des Canadiens et leur nature, ainsi que la quantité d'information diffusée aux gouvernements canadien et étrangers au sujet de Canadiens.

Nous avons également examiné des cas réels pour voir comment les politiques et les procédures sont mises en pratique.

La toile de fond de tout ce travail se composait des constatations de la Commission McDonald et d'un examen que nous avons fait de la réforme du FBI (Federal Bureau of Investigations) qui a eu lieu aux États-Unis au milieu des années 1970. Nous avons rencontré à Washington des agents du FBI et des membres supérieurs du Permanent Select Committee of the House of Representatives on Intelligence et du Senate Select Committee on Intelligence.

Transition

Nous avons examiné les activités de transition, c'est-à-dire les efforts pour orienter le personnel et modifier la politique et les règlements en 1984, année où la *Loi sur le SCRS* est

entrée en vigueur et où le SCRS a assumé les responsabilités en matière de sécurité et de renseignements du service de sécurité de la GRC.

Plus de deux ans après la passation des pouvoirs, la révision des procédures restait incomplète. Le Manuel des opérations était toujours périmé et même, à certains égards, contraire à l'esprit de la *Loi*.

Ce fait était troublant, mais le SCRS est conscient du problème et a entrepris une révision approfondie du Manuel. Nous comptons examiner la nouvelle version dès que possible.

Nous avons appris que le SCRS avait poursuivi toutes les enquêtes du service de sécurité de la GRC examinées en 1984—quoique parfois modifiées pour se conformer à la nouvelle *Loi sur le SCRS* vu les justifications à cet effet. Deux enquêtes examinées seulement à une étape ultérieure ont été abandonnées.

Ressources

L'antisubversion ne bénéficie que d'une proportion relativement faible des ressources du SCRS. Témoignant devant le Comité de la Chambre des communes chargé de la justice et du solliciteur général l'an dernier*, le directeur a évalué cette proportion à «moins de cinq pour cent».

Nous comprenons les raisons de l'évaluation du directeur, mais nous croyons qu'il serait plus juste de parler de «dix pour cent, ou un peu plus, des ressources opérationnelles». Quoi qu'il en soit, il s'agit d'une proportion relativement faible.

Au cours de notre étude, nous avons constaté une certaine frustration parmi les enquêteurs du SCRS qui considéraient que l'antisubversion était la mal-aimée de la famille du SCRS et qu'elle bénéficiait de ressources insuffisantes comparativement au contre-espionnage et à l'antiterrorisme. En fait, nous avons constaté que l'antisubversion semblait parfois servir à satisfaire les besoins urgents en matière de personnel des autres directions opérationnelles. La direction d'antisubversion est en train de prendre les mesures nécessaires pour relever le moral.

Sources humaines

Une section séparée de l'administration des sources humaines dessert toutes les directions opérationnelles. Elle s'intéresse surtout aux sources rémunérées. Elle cherche, par exemple, à s'assurer qu'elles sont fiables. Elle a aussi des règles précisant ce qu'on peut et ce qu'on ne peut pas demander aux sources rémunérées de faire. Mais elle ne prend pas les mêmes précautions à l'égard des sources non rémunérées.

Il n'existe pas de contrôle centralisé de «l'attribution des tâches» qui consiste à dire aux sources, rémunérées et non rémunérées, exactement quelles cibles contrôler et quel type

* Chambre des communes, *Procès-verbaux et témoignages du Comité permanent de la justice et du solliciteur général*, 11 décembre 1986.

d'information est recherché. L'attribution des tâches est la responsabilité des différentes directions opérationnelles.

Ciblage

Le choix des cibles principales aux fins d'enquête est surveillé par un Comité d'approbation et de réévaluation des cibles (CARC) composé de gestionnaires supérieurs du SCRS qui bénéficient des conseils d'un avocat. Comme la Section de l'administration des sources humaines, il dessert toutes les directions opérationnelles.

Vu que le CARC autorise le ciblage pour des périodes précises, il s'occupe des renouvellements aussi bien que des nouvelles cibles.

Il prend ses décisions après avoir examiné les Rapports d'évaluation d'un sujet (RES) établis par les enquêteurs.

Les groupes sont ciblés en vertu de l'article 2 de la *Loi sur le SCRS*. Dans le domaine de l'antisubversion, une influence étrangère indue et la possibilité de violence sont les critères le plus souvent invoqués.

Les particuliers peuvent aussi être ciblés en vertu de l'article 2. Mais la plupart deviennent automatiquement des cibles à cause de leurs rapports avec un groupe ciblé.

Une enquête active n'est pas effectuée sur toutes les cibles. La décision d'enquêter sur un particulier est prise par les gestionnaires des régions ou des directions d'après la menace apparente, l'information prévue dans le plan annuel du SCRS, et l'accessibilité des ressources.

Certains particuliers ciblés font l'objet d'une enquête active (on peut demander un mandat judiciaire en vue d'installer une table d'écoute sur leur téléphone, par exemple) et d'autres, d'une enquête passive (qui peut se réduire dans certains cas à l'accumulation d'articles de journaux à leur sujet).

Comme on peut s'y attendre, des enquêtes seront probablement menées sur les chefs de file des groupes ciblés plutôt que sur leurs membres, et sur leurs membres plutôt que sur leurs partisans. Le terme «chef de file» inclut tant les mentors influents que les personnes qui occupent une charge au sein du groupe ciblé.

Le CARC choisit les catégories de particuliers qui feront l'objet d'une enquête à cause de leurs rapports avec un groupe ciblé.

Mais il existe aussi une autre classe de cibles, qui renferme toutes les personnes ayant des contacts réguliers avec une personne déjà ciblée aux fins d'enquête active par le CARC. Ces cibles de deuxième plan sont déterminées sur le terrain et ne viennent pas du tout à la connaissance du CARC.

Pour un certain nombre de raisons, nous craignons que le filet jeté par le programme d'antisubversion ne soit trop large.

Ciblage selon la catégorie. On pourrait considérer que le CARC cible d'entières catégories de personnes, processus que nous décrivons ci-dessus. Mais on pourrait aussi considérer qu'il cible les particuliers sans tenir compte de la menace, s'il y en a, qu'ils constituent personnellement envers la sécurité du Canada.

Nous croyons que cette dernière méthode n'est pas suffisamment précise. Certains groupes qui subissent tacitement une influence étrangère, par exemple, peuvent inclure seulement quelques membres qui sont conscients de cette influence. Même dans les groupes qui ont des visions radicales de l'avenir, la violence peut être le moyen préféré de quelques membres seulement. Il n'est pas évident que tous les agents de groupes de façade connaissent nécessairement les programmes tacites de ces groupes ou entreprendraient des activités préjudiciables à la sécurité du Canada.

Nous croyons qu'il serait plus utile de déterminer des façons de prévenir ces personnes des objectifs réels de l'organisme (voir la page 34 du présent rapport).

Nous sommes encore plus préoccupés par les cibles de second plan que nous décrivons ci-dessus—soit les personnes ciblées simplement à cause de contacts réitérés avec une personne ciblée.

Tort éventuel. Il s'ensuit de nos observations au sujet du ciblage selon la catégorie que le processus actuel ne tient pas suffisamment compte du tort qui pourrait être fait aux principes de la liberté personnelle et de la vie privée.

Le processus de ciblage ne tient pas compte non plus du tort éventuel qui pourrait être fait à de précieuses institutions sociales, si, par exemple, la surveillance décourageait les adhésions aux associations volontaires qui donnent à leurs membres l'occasion de promouvoir des causes légitimes et de se dévouer à des motifs charitables.

Nous recommandons vivement de toujours inclure dans les RES une description équilibrée des effets—favorables et défavorables— qu'une enquête pourrait avoir sur la liberté individuelle et la vie privée de même que sur l'intégrité des institutions sociales. Les RES que nous avons vus gardaient le silence sur ces questions.

Que constitue une menace? Certaines des menaces décrites par le SCRS sont claires; tous les Canadiens loyaux conviendraient qu'elles méritent l'attention soutenue du Service. Mais certaines nous ont laissés perplexes.

Un RES décrit par exemple «l'attaque» d'un certain organisme contre «le gouvernement anti-communiste pro-américain d'El Salvador ... à l'appui direct ... d'objectifs d'orientation destinés à ... contrarier les initiatives étrangères des États-Unis». Nous ne pouvons admettre qu'une attaque non violente contre la politique étrangère des États-Unis constitue nécessairement une menace envers la sécurité du Canada.

D'autre part, la collecte de fonds au Canada pour les rebelles Contra au Nicaragua paraît n'avoir suscité que peu d'intérêt au SCRS, quoique cette activité paraisse correspondre au critère de l'article 2, à savoir : «les activités ... qui s'y déroulent [au Canada] et visent à

favoriser l'usage de la violence grave ... contre des personnes ou des biens dans le but d'atteindre un objectif politique ... dans un État étranger».

Ce contraste appuie nos craintes (voir la page 27 du présent rapport) que le SCRS est peut-être trop prêt à faire sienne la politique étrangère de nos alliés et à négliger celle du Canada.

Gravité des menaces. Le SCRS semble penser comme nous que bien des groupes ciblés par la Direction de l'antisubversion constituent une menace minime envers le Canada.

Nous reconnaissons que quelques groupes constituent une menace réelle. Toutefois, le SCRS consacre de l'argent et des efforts à trop de cibles d'antisubversion et il s'ingère dans la vie et les activités de trop de Canadiens dans ce secteur.

Recommandations. Nous avons déjà proposé que les RES incluent toujours un exposé du tort que l'enquête pourrait faire aux libertés individuelles et à la vie privée ainsi qu'à l'intégrité des institutions sociales.

De plus, le CARC devrait songer à ne plus cibler d'entières catégories de personnes mais de traiter des particuliers individuellement. Les RES devraient alors justifier une à une les enquêtes sur les particuliers.

Nous suggérons que les RES comprennent aussi une description explicite a) de la gravité de la menace, b) de son imminence, c) du besoin du type d'enquête envisagée comparativement à des techniques comportant moins d'intrusion et d) de l'objet de l'enquête.

Ils devraient être moins fondés sur des incidents isolés et donner davantage un exposé cohérent des raisons militant en faveur de la décision de ciblage recherchée de la part du CARC.

Dans le même esprit, nous serions plus tranquilles si des efforts plus vastes étaient déployés afin d'assurer que toutes les demandes de mandats judiciaires donnent également les raisons qui militent contre l'exercice des pouvoirs comportant intrusion (voir la page 11 du présent rapport).

Le SCRS devrait tenir un fichier complet et à jour des particuliers susceptibles de faire l'objet d'une autorisation d'enquête, plutôt que le fichier partiel qui existe actuellement.

Dossiers sur des particuliers

Des dossiers sont ouverts sur des particuliers et des organismes ciblés. Nous avons été incapables de déterminer le nombre précis de dossiers ouverts par suite des opérations d'antisubversion, vu que ces dossiers ne sont pas séparés de ceux sur le contre-espionnage et l'antiterrorisme.

D'après les meilleures informations que nous avons pu recueillir, la Direction de l'antisubversion a probablement plus de 30 000 dossiers, au bas mot, sur des particuliers. Cela nous inquiète un peu : nous n'avons pas de chiffres exacts et nous ne pouvons pas en obtenir sans l'examen de milliers de dossiers.

Des enquêtes actives ont été entreprises sur seulement un petit pourcentage de ceux-ci.

Pour mettre davantage ces 30 000 dossiers en contexte, précisons que le SCRS dans son ensemble détient plus de 600 000 dossiers sur des particuliers.

(Il a ouvert 112 000 dossiers semblables en 1986-1987. Ils comprennent des dossiers administratifs sur, par exemple, les propres employés du Service ainsi que des dossiers sur les évaluations de sécurité et l'immigration, dont il y a une rotation rapide.)

Malgré des efforts au début des années 1980 pour purger les dossiers d'une valeur limitée ou nulle pour le renseignement, le nombre de dossiers sur des particuliers dans le domaine de l'antisubversion semble être demeuré relativement stable si on le compare au nombre de dossiers détenus par le prédecesseur du SCRS, le service de sécurité de la GRC.

Vieux dossiers. De nombreux dossiers actuellement détenus ont été ouverts lorsque le renseignement de sécurité était la responsabilité du service de sécurité de la GRC, avant que ne soient formulées la définition légale de «menaces envers la sécurité du Canada» (article 2 de la *Loi sur le SCRS*) et la règle du «strictement nécessaire» (article 12).

Nous avons déjà indiqué clairement dans le présent rapport (page 26) qu'à notre avis le SCRS devrait rouvrir ses dossiers sur les particuliers et en radier l'information qui ne correspond pas aux normes énoncées aux articles 2 et 12.

Nous suggérons également que des critères détaillés soient élaborés concernant l'ouverture de dossiers sur des particuliers et des groupes et que la mise en oeuvre de ces critères soit revue périodiquement.

Diffusion de l'information

Lorsque nous avons demandé au SCRS combien d'informations étaient fournies aux organismes des gouvernements canadien et étrangers, il nous a répondu que le système de gestion de l'information ne pouvait pas facilement donner de tels détails. Chaque dossier montre l'information fournie aux différents organismes. Mais il n'existe pas de codage nous permettant d'obtenir des chiffres d'ensemble sans procéder à une recherche dans chaque dossier.

Cette lacune pourrait rendre plus difficile l'exercice de nos fonctions de contrôle en vertu des articles 17 et 19 de la *Loi sur le SCRS*, qui portent sur l'échange d'information.

Nous recommandons de programmer le système de gestion de l'information de façon à permettre un accès immédiat aux statistiques d'ensemble sur l'information transmise à destination et en provenance des organismes des gouvernements canadien et étrangers.

En outre, il faudrait élaborer une politique et une procédure de vérification spécifiques régissant la diffusion de toute information sur un résident canadien.

Cinq organismes

Nous avons examiné les dossiers opérationnels de cinq organismes représentant différentes catégories de cibles d'antisubversion, afin de déterminer si des enquêtes sur ces groupes étaient justifiées en vertu des articles 2 et 12 de la *Loi sur le SCRS*.

Nous avons comparé les dossiers avec les RES pertinents et avec les affidavits applicables à l'appui des mandats judiciaires, et nous avons discuté de nos impressions avec les experts du SCRS.

En faisant notre propre évaluation des efforts d'enquête du Service par rapport à chacune de ces cibles, nous avons tenu compte des exigences de la *Loi sur le SCRS*, de la gravité et de l'imminence de la menace comme nous la voyions, et de l'importance des ressources que le SCRS y affectait.

Nous avons conclu que la Direction de l'antisubversion s'occupe principalement de deux questions :

- L'aptitude éventuelle des puissances étrangères à manipuler la politique canadienne par le truchement d'institutions sociales ou de groupes de protestation légitimes.
- La possibilité que certains groupes puissent miner les institutions canadiennes et renverser l'État par la violence.

Dans les deux cas, on semblait croire le public canadien beaucoup trop facile à duper.

Nous estimons que la Direction de l'antisubversion surestime l'influence et le pouvoir de persuasion de ces groupes. D'après notre propre interprétation des médias et notre connaissance personnelle de particuliers de toutes conditions sociales, nous savons que les Canadiens sont généralement assez adultes pour ne pas se laisser séduire par les groupes concernés.

Surestimation. Nous croyons aussi que le SCRS surestime la possibilité de violence par certains groupes.

Un groupe ciblé, par exemple, publie une revue qui traite d'un vaste éventail de questions, des arts à la politique sociale, d'après la perspective de l'extrême gauche.

Il est vrai que certains membres préconisent l'usage de la violence par ce groupe, mais ils ont été écartés par les autres.

Il pourrait y avoir lieu d'enquêter sur les partisans de la violence dans ce groupe en tant que particuliers.

Mais nous ne sommes pas encore convaincus que le groupe lui-même devrait être ciblé aux fins d'enquête. Cela laisserait la porte ouverte à une ingérence inutile dans les libertés et la

vie privée tant des membres les plus anodins que des membres les plus odieux. Cela pourrait aussi nuire à la liberté d'expression, une de nos valeurs sociales les plus prisées.

Pour conclure, n'importe quel groupe ciblé pourrait éventuellement se livrer à des actes terroristes mais, d'après la preuve accessible, la plupart ne le feront probablement pas dans un avenir prévisible.

Deux champs d'action

La zone d'ombre où opère la Direction de l'antisubversion se scinde en deux champs d'action qui correspondent à ses deux principales préoccupations : l'influence étrangère indue et le risque de violence.

Ces préoccupations se trouvent être les responsabilités respectives de ses deux directions apparentées, celles du contre-espionnage et de l'antiterrorisme.

Nous recommandons de délimiter ces deux champs d'action et de partager le rôle d'antisubversion entre ces deux directions. Ainsi, la Direction du contre-espionnage serait chargée de l'influence étrangère indue et la Direction de l'antiterrorisme, du risque de violence.

Les priorités seraient plus rationnelles et certains des groupes ciblés que nous mentionnons ici apparaîtraient plus clairement sous leur vrai jour.

Et les bons agents de renseignements qui peuvent maintenant se sentir isolés et mal appréciés dans leur rôle d'antisubversion se trouveraient dans un environnement plus actif où ils pourraient donner libre cours à leurs talents.

7. Le SCRS lui-même

Après avoir exposé nos conclusions sur le contrôle, nous revenons à l'une des questions que nous posions au chapitre 2 : Le SCRS est-il efficace, en ce qui concerne à la fois des objectifs administratifs comme l'intégrité financière et des objectifs d'orientation comme la transformation en organisme civil et le bilinguisme officiel? Comme il fait l'objet d'une enquête spéciale, le bilinguisme officiel sera traité dans le prochain chapitre. Ce dernier est centré sur d'autres questions internes.

Ressources et administration

L'obligation de dépenser l'argent public sagement doit toujours constituer une priorité, et elle est doublement impérative pendant la période de restrictions actuelle. Toutes les instances gouvernementales, y compris le SCRS, sont financièrement à l'étroit.

Mais le SCRS a aussi des problèmes qui lui sont propres. Il n'a pas fini de payer les frais ponctuels «de transition» occasionnés par la création d'installations et de services qui relevaient déjà de la GRC. Ces frais de démarrage se sont parfois révélés plus élevés que prévu.

Le Service a également été appelé à assumer de nouvelles tâches sans être déchargé de ses anciennes et, dans certains cas, sans obtenir un complément d'argent ou de personnel. À ce sujet, nous avons salué la décision gouvernementale d'affecter en 1986-1987 une somme importante à l'amélioration du programme d'antiterrorisme. Nous espérons que l'on continuera de veiller à ne pas surcharger le SCRS de travail.

Logement. Les restrictions ont entravé le programme par lequel le SCRS comptait fournir à tout son personnel des bureaux distincts de ceux de la GRC. Ironie du sort, un de leurs effets a été d'augmenter les coûts ultimes, à tout le moins en dollars courants, à cause d'une inflation relativement légère mais persistante. Dans certains cas, l'incapacité du SCRS de quitter les logements de la GRC à temps a pu contribuer à refroidir les relations entre ces deux organismes.

Par suite d'un rapport du vérificateur général concernant les retards et les dépassements de coûts dans la rénovation des lieux de travail à Montréal, le SCRS rédige ses propres lignes directrices et politique concernant le logement pour remplacer celles de la GRC qu'il utilisait. Inutile de dire que nous applaudissons à cette initiative.

SGST. Dans le rapport de l'an passé, nous nous sommes plaints de lacunes dans les documents du SCRS relatifs au SGST (Système de gestion du secteur de dépenses).

Le SCRS a pris des mesures positives depuis lors. Dans le POP (Plan opérationnel pluriannuel) de l'automne dernier, il s'est servi de sous-éléments qui correspondent plus étroitement au rendement opérationnel (toutefois, comme certains de ces sous-éléments ne peuvent être liés à des unités organisationnelles distinctes, il est difficile de connaître le gestionnaire responsable). Il essaie aussi de montrer l'incidence marginale des dépenses en matière de sécurité lorsqu'il demande des fonds.

En revanche, nous estimons que, même si le SCRS répond pleinement aux exigences du Conseil du Trésor, les derniers POP contiennent moins de renseignements que les précédents.

Aux fins de notre propre analyse, nous voulions en savoir davantage, et les renseignements que nous a fournis le SCRS nous ont permis d'examiner les dépenses aussi à fond que par les années passées. Nous ne manquerons pas de demander ces renseignements à l'avenir.

Transformation en organisme civil

Une des critiques les plus sérieuses formulées à l'égard du service de sécurité de la GRC était qu'il apportait une approche policière au travail de sécurité de renseignements.

Les différences sont de taille. Comme l'a noté une étude, le travail de sécurité «offre peu des certitudes sociales et légales» que la police peut trouver dans les «objectifs comparativement clairs que constituent la prévention et l'appréhension»*. Nous avons déjà indiqué, par exemple, nos propres inquiétudes touchant l'incidence de l'approche policière cas-par-cas sur l'effort de recherche du SCRS (page 16).

L'objet du travail de sécurité de renseignements n'est pas essentiellement de mettre les mécréants derrière les barreaux. Le mandat fondamental du SCRS est exposé dans la *Loi sur le SCRS* qui dit (à l'article 12) que le Service :

> recueille [...] et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.

La Commission McDonald, comme la Commission Mackenzie une décennie environ avant elle, a recommandé la création d'une agence civile de sécurité de renseignements qui serait distincte de la GRC. La «transformation en organisme civil» est devenue l'un des objectifs d'orientation sous-tendant la *Loi sur le SCRS* adoptée par le Parlement en 1984.

Service dévoué. Pour de nombreuses raisons, le SCRS continuera pendant bien des années à montrer ses origines policières. Facteur important, le service de sécurité de la GRC avait la seule vaste réserve de personnel formé dans laquelle il pouvait puiser.

On ne peut pas reprocher au SCRS d'avoir choisi un grand nombre de ses agents de renseignements (AR) parmi le personnel du service de sécurité; la transformation en organisme civil est un objectif pour aujourd'hui et demain, et elle ne porte pas atteinte au travail inestimable effectué par des hommes et des femmes dévoués qui ont débuté leur carrière au sein du service de sécurité. De plus, il était normal pour le SCRS de se prévaloir de certains services et installations de la GRC. Il ne serait pas réaliste de s'attendre à autre chose.

---

* Richard French et André Béliveau, *The RCMP and The Management of National Security* (Montréal, L'Institut de recherches politiques, 1979), page 4.

Néanmoins, nous ressentons le besoin réel de continuer à aiguillonner le SCRS le long de la voie qui mène à sa transformation en organisme civil. Le Tableau 2 montre la distance qu'il reste à parcourir.

Tableau 2. Composition de l'ensemble du personnel du SCRS

Anciens membres en uniforme de la GRC	46 %
Anciens membres civils de la GRC	15 %
Anciens fonctionnaires travaillant pour la GRC	21 %
Employés qui n'ont jamais travaillé pour la GRC	17 %

(Source : chiffres fournis le 3 décembre 1986 par le SCRS)

Le SCRS semble croire que les chiffres constituent une bonne réponse à ceux qui affirment qu'il ne s'agit que de la GRC sans son Carrousel; moins de la moitié de ses employés étaient déjà des membres en uniforme de la GRC, signale-t-il.

Nous voyons les choses autrement : plus de 80 pour cent des gens qui travaillent pour le SCRS ont apporté de la GRC leurs souvenirs et leurs habitudes de travail. Même si nous n'avons pu encore obtenir de chiffres exacts du SCRS, nous n'avons pas le moindre doute que cette proportion est encore plus élevée dans la catégorie clé des AR et au palier de la gestion intermédiaire.

Ces données s'appliquent à la période qui a suivi le «délai de grâce». En effet, pendant les deux années qui se sont terminées le 16 juillet 1986, les anciens membres de la GRC avaient le droit de réintégrer la Force, et 75 l'ont fait, soit une proportion relativement faible des bénéficiers de ce droit.

Provenance des recrues

Le recrutement de l'extérieur pour tous les niveaux est la façon de changer cet état de choses. Nous sommes sérieusement préoccupés par l'accent que le SCRS a mis jusqu'à présent dans son recrutement sur les «admissions directes», comme le montre le Tableau 3.

Tableau 3. Provenance des nouveaux AR de janvier 1985 à décembre 1986

Recrutement public	51 %
Admissions directes (surtout des forces policières	34 %
Conversions au sein du SCRS	15 %

(Source : statistiques fondées sur les chiffres du SCRS)

Près de la moitié des nouveaux AR embauchés en 1985 et 1986 avaient des antécédents policiers. Les admissions directes sont les personnes qui ont une expérience de forces policières, des militaires et d'autres secteurs et qui accèdent au poste d'AR sans avoir reçu la

formation de base à l'Académie Sir William Stephenson du Service. Les conversions sont d'anciens surveillants qui ont commencé leur carrière dans la GRC à titre d'«agents spéciaux».

Le Tableau 4 montre que la catégorie des «employés qui n'ont jamais travaillé pour la GRC» au Tableau 2 inclut d'anciens policiers d'autres forces, et il donne aussi d'autres détails pertinents.

Tableau 4. Recrues AR exemptées de formation à l'Académie Sir William Stephenson entre janvier 1985 et décembre 1986

Source	Sexe		Langue maternelle		Niveau d'admission	
	M	F	Fr	Angl	AR-2	AR-3
GRC	33	6	6	33		39
MDN	2			2		2
BCP	1			1		1
CEIC		1		1		1
Autres forces policières	5		1	4	1	4
Total	41	7	7	41	1	47

(Source : SCRS)

En tant que bon employeur, le SCRS devrait continuer d'intégrer dans la catégorie des AR des surveillants et d'autres employés ayant les qualités requises, mais nous croyons qu'il devrait insister sur d'autres facteurs que l'expérience des enquêtes policières dans son recrutement.

La collecte d'informations ne constitue qu'un aspect du travail. Le genre d'information dont s'occupe le SCRS est seulement aussi valable que l'analyse qui en est faite et les conseils que le gouvernement reçoit par la suite. L'accent doit être mis sur une solide formation universitaire dans le domaine de la recherche et des sciences sociales.

Nous avons aussi découvert que les diplômés de l'Académie qui commencent à travailler au niveau AR-1 n'apprécient pas que les «admissions directes» soient nommées au niveau «de compagnon» AR-3 (voir la page 52).

L'Académie ferme ses portes

Les déclarations écrites du Service en réponse à l'une de nos questions officielles nous ont rassurés pendant quelques courtes semaines. Il affirmait qu'il ne s'attendait pas à d'autres

admissions directes aux niveaux AR-2 et AR-3 et que tous les nouveaux AR—sauf ceux qui figuraient déjà sur la liste de paye à d'autres titres—passeraient par l'Académie.

Mais nous avons été subséquemment stupéfaits d'apprendre que le SCRS avait embauché 16 anciens policiers pendant le dernier trimestre de 1986 et qu'il n'avait laissé aucun poste vacant pour des recrues universitaires ou civiles.

Par conséquent, l'Académie a été fermée pour un an, et la transformation du Service en organisme civil marque un temps d'arrêt.

Nous croyons comprendre que la réouverture de l'Académie est prévue pour 1988. Nous recommandons vivement qu'une attention plus soutenue soit accordée à la transformation en organisme civil et que, à cette fin, aucun nouvel employé ne soit admis directement des forces policières afin qu'une nouvelle classe de recrues civiles puisse être constituée aussitôt que possible.

Bilinguisme et participation équitable

La classe de 1987-1988 devait être la première dont chaque membre serait bilingue—comme la direction du SCRS l'avait solennellement décidé il y avait quelques mois et comme nous l'avons recommandé.

Elle aurait également offert au Service l'occasion de suivre nos recommandations réitérées et de prendre des mesures en vue d'augmenter la proportion de femmes et de francophones à l'intérieur de la main-d'oeuvre.

Le Tableau 5 montre clairement pourquoi il importe de répéter ces recommandations et pourquoi la classe de 88 sera si vivement regrettée.

Tableau 5. Caractéristiques choisies des recrues du SCRS constituant les trois premières classes à l'Académie Sir William Stephenson (pourcentages)

	Janvier 1986	Juin 1986	Février 1987
Recrues bilingues (anglais-français)*	9	10	10
Femmes	25	20	10
Recrues dont la première langue officielle est le français	3	10	10

(Source : SCRS)

* Le SCRS a précisé qu'un autre tiers de la première classe, que tout le reste de la deuxième classe et que près du tiers de la dernière classe étaient composés d'anglophones possédant «une certaine connaissance» du français.

La première classe

Dans notre dernier rapport annuel, nous avons discuté de notre rapport intitulé *Dix-huit mois après la séparation : une appréciation de la conception du SCRS sur le recrutement, le perfectionnement et les questions connexes*. Pendant la recherche, nous avons questionné les premières recrues civiles, qui étaient alors en formation à l'Académie. Nous avons trouvé que leurs impressions du programme de formation étaient généralement favorables.

En 1986-1987, nous avons tenu une entrevue de suivi avec près de la moitié des diplômés de la première classe. Sauf les exceptions mentionnées ci-dessous, le moral restait bon.

En général, les membres de la première classe aimaient leur travail, le trouvaient intéressant, et étaient satisfaits de leurs fonctions et de leur perfectionnement. Sur une échelle de un à cinq, ils ont attribué en moyenne la cote quatre à leurs sentiments au sujet du SCRS. La plupart ont indiqué qu'ils s'attendaient à faire carrière au sein du SCRS et ils ont coté leurs occasions d'avancement quatre sur une échelle allant jusqu'à cinq.

Admissions directes. D'après presque tous ceux que nous avons questionnés, la seule ombre au tableau était qu'un traitement préférentiel avait été accordé aux admissions directes— c'est-à-dire aux agents de renseignements qui sont admis directement au SCRS parce qu'ils ont une expérience de la police.

Les recrues admises directement ne sont pas tenues de suivre le cours d'introduction à l'Académie et elles sont généralement embauchées au niveau AR-3 (voir le Tableau 4 ci-dessus), alors que les recrues civiles sont embauchées au niveau AR-1.

Cela représente un écart de traitement d'environ 10 000 $ par année, même si les fonctions d'un AR-3 et d'un AR-1 sont essentiellement les mêmes. Cette différence de niveau est fondée sur la supposition que les AR-3 sont des employés chevronnés sur lesquels on peut compter pour travailler davantage en autonomie et même pour épauler les AR-1.

Les AR-1 sont frustrés par cette situation—à telle enseigne que nous craignions de perdre de bons éléments parce qu'ils avaient l'impression de commencer leur carrière avec un handicap.

Dans un autre ordre d'idées, l'avantage accordé aux admissions directes semble perpétuer la domination du Service par des gens qui ont fait leurs premières armes au sein d'organismes policiers.

Pour ces deux raisons, nous nous réjouissons des nouveaux arrangements qui permettront aux AR-1 supérieurs (habituellement des diplômés civils de l'Académie) d'atteindre le premier niveau de gestion (AR-4) dans guère plus de sept ans—et non dans les onze ans prévus à l'origine. Mais ce délai est toujours beaucoup plus long que les deux ans dans lesquels un AR-3 (anciens policiers admis directement) peut espérer devenir AR-4.

Formation. La première classe avait diverses observations à faire sur l'utilité, dans son travail de tous les jours, de la formation qu'elle avait reçue à l'Académie. Sa suggestion prin-

cipale était que, tout compte fait, la formation devrait être davantage axée sur des besoins quotidiens comme la manipulation des sources, les entrevues et la rédaction des rapports.

Amélioration du moral

Nous croyons qu'il y aurait lieu de lancer une campagne de relations publiques destinée à sensibiliser les Canadiens au SCRS et à son rôle. À notre sens, cela aurait un effet marqué sur le moral et donnerait aux employés du SCRS une image de marque positive qui appuyerait leur propre croyance en leur contribution personnelle à la sécurité du Canada.

L'acquisition d'une image forte et positive par le SCRS comblerait aussi tout fossé entre la formation des anciens policiers et celle des employés qui se sont initiés au travail du renseignement de securité dans l'atmosphère moins militaire du SCRS.

Utilisation du polygraphe

L'utilisation du polygraphe est une autre question liée au recrutement. Malgré une bonne nouvelle, nous sommes déçus de l'inaction du SCRS et du ministère du Solliciteur général à cet égard.

Dans notre dernier rapport annuel, nous exposions en détail nos sérieuses réserves sur l'usage que le Service faisait du polygraphe (appelé faussement «détecteur de mensonges» par le public) pour filtrer les employés éventuels et vérifier la loyauté des employés existants.

Témoignant devant le Comité permanent de la Chambre des communes chargé de la justice et du solliciteur général*, le directeur a affirmé qu'il n'était pas convaincu que l'avis exprimé par nous-mêmes et par d'autres soit «suffisamment solide pour justifier l'abandon de cet outil d'enquête». Il a noté en particulier que le polygraphe ne constitue qu'une des 21 étapes du processus de recrutement et que tout doute qu'il pourrait susciter fait l'objet d'une enquête par la suite.

«Je pense que nous aurions tort d'utiliser le polygraphe comme seul et unique moyen de déterminer si une personne est réticente ou ne dit pas la vérité, et nous ne le ferions pas», a-t-il dit au Comité.

Fausse apparence. Nous croyons avoir réfuté cet argument l'an passé en affirmant que nous ne pouvions pas croire que le SCRS puisse s'en tenir à sa politique consistant à ne pas se servir des résultats du polygraphe comme motif unique pour refuser une habilitation de sécurité. À cause de leur fausse apparence de rigueur scientifique, les résultats du polygraphe seraient le plus souvent pris pour argent comptant. La tentation serait forte de ne pas tenir compte d'un résultat contraire des enquêtes qui, elles, sont sujettes à l'«erreur humaine».

* Chambre des communes, *Procès-verbaux et témoignages du Comité permanent chargé de la justice et du solliciteur général*, 11 décembre 1986.

Voici les principaux arguments que nous invoquions l'an dernier :

- Il n'existe aucune étude scientifique généralement acceptée qui établit la valeur du polygraphe pour l'embauchage et le filtrage de sécurité en bloc (même si nous reconnaissons que le polygraphe peut constituer l'un des nombreux outils utilisés pendant une enquête criminelle).
- Même les défenseurs du polygraphe admettent que les résultats sont parfois faux—au moins 10 pour cent du temps. Tout rédacteur qui ferait autant de fautes d'orthographe se retrouverait sans emploi, et pourtant les lectures de polygraphe dont le taux d'exactitude est inférieur à 90 pour cent sont taxées de «scientifiques» et peuvent coûter aux Canadiens leurs carrières et leurs réputations. À vrai dire, à cause de son taux d'erreur, le polygraphe ne peut même pas être considéré comme une protection étanche contre l'infiltration du Service par des personnes déloyales et malhonnêtes.
- Même si les membres actuels du SCRS n'étaient pas tenus de se soumettre à des tests, nous ne croyions pas que l'administration de ceux-ci puisse être vraiment volontaire, comme l'avait affirmé le Service. Toute personne montrant des réticences à ce sujet serait forcément soupçonnée d'avoir quelque chose à cacher, et les pressions pour l'obliger à consentir au test serait tellement fortes que seuls les plus déterminés pourraient y résister.
- Enfin, nous craignions que l'usage du polygraphe ne se répande au gouvernement s'il devenait pratique courante au sein du Service, semant sur son passage crainte et méfiance—valeurs négatives à favoriser dans un pays comme le nôtre.

La bonne nouvelle est que depuis lors le SCRS a mis un terme aux tests «volontaires» qu'il administrait à ses employés déjà en poste. Voilà qui lève une des objections que nous formulions dans notre dernier rapport annuel.

Mais le SCRS et le ministère du Solliciteur général n'ont pas encore dissipé le reste de nos doutes.

Un déguisement. Subir le test du polygraphe constituait toujours une condition d'emploi pour les recrues, qui devaient répondre à des questions liées à leur mode de vie et à leur loyauté. Le SCRS a tenté de donner à son programme un vernis scientifique en le qualifiant de projet pilote, mais il s'agit là simplement d'un déguisement.

Le terme «projet pilote» suggère une expérience soigneusement planifiée et aussi soigneusement évaluée. Or, le programme du SCRS ne comporte aucun mandat ni aucune méthode d'évaluation élaborés avant les tests. En un mot, il n'y a pas de «projet pilote», mais seulement la poursuite des mêmes vieux tests du polygraphe sous une nouvelle étiquette.

Entre-temps, le ministère du Solliciteur général n'a pas activement donné suite à cette question.

Le personnel ministériel nous a informés qu'il attendait les résultats de deux études en cours dans d'autres pays. Intéressés nous-mêmes par ces études, nous avons fait enquête et appris que l'une avait été annulée et que l'autre n'avait donné aucun résultat utile. Nous avons prévenu le Ministère en conséquence.

Sur les conseils d'un comité interministériel, le Ministère s'est contenté d'obtenir une opinion juridique, voulant que les tests du polygraphe puissent être considérés comme une condition légale d'emploi.

Lacune essentielle. Cela ne comblait toujours pas la lacune essentielle des tests du polygraphe, soit leur manque de fiabilité et les injustices qui peuvent découler d'erreurs commises pendant la lecture de leurs résultats.

Nous avons entendu des rapports que les agences de sécurité et de renseignements de pays amis peuvent exercer certaines pressions sur le SCRS pour qu'il se serve du polygraphe pendant le filtrage de sécurité. Nous croyons qu'il devrait résister à ces pressions en l'absence d'une preuve concluante que le polygraphe est plus fiable qu'on ne le croit généralement.

En fait, nous estimons que des enquêtes rigoureuses conçues pour le filtrage de sécurité et l'embauchage rendraient l'utilisation du polygraphe superflue de toute façon.

Et nous préconisons encore une fois, comme nous l'avons fait dans notre dernier rapport annuel, l'arrêt des tests effectués avec le polygraphe aux fins de l'embauchage et du filtrage de sécurité et la réalisation d'une étude appronfondie et objective qui permettrait au solliciteur général et au gouvernement de décider pour eux-mêmes si l'utilisation de pareilles méthodes est compatible avec les valeurs d'une société libre et démocratique.

8. Combler les fossés

Comme la transformation en organisme civil que nous étudions dans le dernier chapitre, le bilinguisme officiel constitue un objectif d'orientation majeur de tous les organismes fédéraux, et particulièrement du SCRS qui a bien du retard à rattraper.

En 1986-1987, à la demande du solliciteur général, nous avons étudié à fond le bilinguisme officiel et les relations de travail au sein du SCRS, en nous concentrant sur la région du Québec, la région d'Ottawa et l'Administration centrale, où il semblait y avoir le plus de tensions.

Culture et communications. Notre rapport, présenté au solliciteur général en mars 1987, met en lumière des lacunes en matière de culture et de communications et présente en tout 48 recommandations détaillées destinées à les réduire. La direction du SCRS a entrepris de déployer des efforts conscients et soutenus afin de les combler définitivement. Pour fournir un cadre général, nous avons recommandé :

- Qu'un sous-directeur, Projets spéciaux, soit nommé pour deux ans en vue de surveiller la mise en oeuvre d'un plan spécial relatif aux langues officielles et de nos recommandations destinées à améliorer les relations de travail.
- Qu'un comité consultatif d'experts—provenant du Conseil du Trésor, du Secrétariat d'État et peut-être du secteur privé—soit créé pour aider à mettre le plan en oeuvre.

Nous avons préparé un abrégé du rapport qui bénéficiera d'une vaste diffusion, et nous avons été informés qu'il serait rendu public. Comme nous le disons dans la préface : «Nous espérons que cette attitude manifeste l'intention du Service d'enterrer le fossé et de s'attaquer aux tâches de reconnaître aux langues officielles la place qui leur revient et d'ouvrir la voie aux communications au chapitre des relations de travail*».

Nous continuerons de suivre de près la question des langues officielles et des relations de travail.

Dans le présent chapitre, nous examinons certaines de nos conclusions les plus importantes et formulons d'autres recommandations majeures.

Langues officielles

Nous avons déterminé dans notre étude spéciale que, malgré de bonnes intentions au sommet, il y a eu trop peu d'engagement réel de la part de certains intervenants clés envers la politique des langues officielles du gouvernement ainsi qu'une compréhension insuffisante de la culture francophone qui moule la pensée d'un Canadien sur quatre.

Le SCRS prenait des mesures en vue d'améliorer la situation. Pendant notre enquête :

- Il a levé un moratoire sur la formation linguistique et sur l'obligation qui incombe habituellement aux fonctionnaires unilingues d'apprendre la deuxième langue dans les deux années suivant leur nomination à un poste bilingue.

* *Pour corriger une situation ... Langues officielles et Relations de travail au sein du Service canadien du renseignement de sécurité* (Ottawa, 1987).

- Il a embauché un chef des langues officielles, qui s'est immédiatement mis au devoir pour rédiger des politiques clés.

Nous applaudissons à ces initiatives. Mais des fautes qui ternissent notre optimisme continuent d'être commises.

En fait, nous avons du mal à ne pas succomber à un peu de cynisme depuis que deux décisions mal assorties ont été prises dont l'une au sujet de l'Académie Sir William Stephenson, où sont formés les nouveaux agents de renseignements.

Pendant notre enquête, la direction a décidé que, dorénavant, toutes les recrues admises à l'Académie seraient bilingues et les cours seraient donnés dans les deux langues officielles. Plus tard (voir la page 50 du présent rapport annuel), il a miné sa crédibilité en suspendant les cours à l'Académie pour un an.

Erreur survenue pendant l'enquête même, un guide de la rédaction des directives a été publié en anglais seulement—malgré le principe fondamental que les employés dont la langue de travail est le français ont droit à la même assistance lorsqu'ils exercent leurs fonctions que ceux dont la langue de travail est l'anglais.

Fossé culturel. Voici un petit exemple fort éloquent de ce que nous entendons par le «fossé culturel» : certains anglophones semblent croire que les besoins des francophones peuvent être relégués au second plan. Nous tenons à préciser que cette approche n'était pas universelle, mais nous en avons découvert des traces trop souvent à notre goût.

Des plaintes concernant des messages qui sont parvenus à la région du Québec en anglais seulement ou en anglais d'abord, une traduction française devant suivre, parfois beaucoup plus tard, comptaient parmi les facteurs qui ont donné lieu à notre enquête. Pourtant, de tels messages sont demeurés un problème à tout le moins jusqu'en octobre 1986—sept mois après le début de notre enquête.

Les messages en anglais seulement de l'Administration centrale enfreignaient clairement la politique des langues officielles applicable dans l'ensemble du gouvernement. Officiellement désigné à titre de bureau bilingue dont le français est la première langue de travail, la région du Québec a le droit de recevoir des communications de l'Administration centrale soit en anglais et en français simultanément ou en français seulement.

Esprit du bilinguisme. Les fréquents messages en anglais seulement d'une section de la région d'Ottawa à la région du Québec étaient, à strictement parler, admissibles en vertu des politiques relatives aux langues officielles. Désignée bureau bilingue elle-même, la région d'Ottawa est justifiée de communiquer avec tous les autres bureaux du SCRS dans l'une ou l'autre des deux langues officielles.

Cependant, nous considérons que la section en question constitue un cas spécial parce qu'elle fournit un service national à toutes les directions du SCRS d'un océan à l'autre, et que l'esprit du bilinguisme officiel exige plus que le strict minimum.

Nous avons souvent entendu l'argument de «l'urgence», à savoir que la traduction en français imposerait des délais inacceptables. À notre avis, cet argument n'était habituellement qu'un prétexte. Par exemple, nombre de textes dans une langue étrangère sont traduits en anglais; pourquoi ne pourraient-ils pas être traduits en français en même temps?

Autres questions. Les autres questions comprennent le niveau très modeste de bilinguisme exigé pour certains postes à l'Administration centrale, le fait que des postes vacants ont été annoncés avant que le chef des langues officielles ait approuvé leurs exigences linguistiques et le défaut d'obtenir une proportion équitable en choisissant la première classe à l'Académie Sir William Stephenson, avec le résultat que seulement une des recrues était francophone («Nous avons gaffé», a reconnu une source haut placée).

Craintes des anglophones. En même temps, nous avons noté que certains employés unilingues anglophones craignaient que la stricte application des politiques linguistiques du gouvernement ne freine leur carrière.

Nous estimons que c'est grâce à des programmes accélérés de formation linguistique que le SCRS prouvera qu'il offre des chances égales à toutes les personnes qualifiées, sans égard—pour reprendre le libellé de la *Charte canadienne des droits et libertés*—à la race ni à l'origine nationale ou ethnique.

Recommandations. Voici certaines des principales recommandations que nous avons présentées concernant les langues officielles :

- Qu'un plan biennal spécial visant les langues officielles soit mis en oeuvre pour rattraper le temps perdu.
- Que le SCRS élargisse en priorité ses installations pour la traduction en français de façon que l'efficience opérationnelle («l'urgence») ne puisse plus être citée pour excuser l'unilinguisme anglais des communications écrites.
- Que la section susmentionnée de la région d'Ottawa ait comme politique de communiquer en français avec les bureaux francophones et les bureaux bilingues dont le français est officiellement désigné comme la première langue de travail.
- Qu'une version française du guide de la rédaction des directives et d'autres guides ou manuels qui existent actuellement en anglais seulement soit publiée en 1987.
- Que des mesures soient prises en vue d'assurer que les postes de gestion sont désignés bilingues sur la même base que dans l'ensemble du gouvernement et qu'aucun concours ne soit lancé avant que le chef des langues officielles ait établi les exigences en matière de langues officielles des postes en question.
- Que l'on prévoie de donner une formation linguistique à tous les employés unilingues occupant des postes bilingues avant la date d'expiration du Plan spécial et que le SCRS décide officiellement d'ici le 31 juillet 1987 ce qu'il fera des employés unilingues qui occupent des postes bilingues et qui a) ne sont pas admissibles à une formation dans la deuxième langue, b) refusent ou négligent de s'inscrire à une telle formation, c) échouent à cette formation ou d) perdent leur capacité de travailler dans la deuxième langue.

- Que l'on continue d'insister sur le bilinguisme en tant que critère de recrutement et que le SCRS élabore des procédures d'embauchage et de dotation propres à assurer un recrutement suffisant de francophones.
- Que la prime de bilinguisme soit versée conformément aux règles du Conseil du Trésor.

Haig-Brown. Parce qu'il y a eu des reportages dans les médias concernant le rapport Haig-Brown, comme il est appelé, il pourrait être utile de présenter brièvement les conclusions que nous avons tirées dans le cadre de notre enquête.

Ce rapport est un recueil de notes de service rédigées par deux officiers de l'Armée affectés à la GRC pendant la Deuxième guerre mondiale pour donner des conseils sur l'organisation de la sélection du personnel. Il perpétue des stéréotypes inacceptables au sujet de certains groupes ethniques.

Les protestations que le Rapport Haig-Brown n'était pas pertinent à son époque ne nous ont pas entièrement convaincus, mais, en analyse finale, nous avons convenu que son intérêt actuel est historique; rien ne prouve qu'il n'ait jamais guidé la sélection du personnel au SCRS.

BCLO. Ajoutons pour mémoire que nous avons mené notre enquête avec la collaboration du Bureau du commissaire aux langues officielles (BCLO), qui effectuait simultanément sa propre vérification des pratiques en matière de langues officielles au SCRS. Le BCLO publiait son propre rapport.

Relations de travail

Nous avons constaté que les problèmes véritables causés par les relations de travail avaient été amplifiés par un fossé de communications dans lequel les gestionnaires et divers employés en étaient venus à croire le pire les uns des autres.

Les problèmes autant que le fossé de communications remontent tous deux en partie à la période de transition entre l'ancien service de sécurité de la GRC et l'actuel SCRS. Les gestionnaires du SCRS eux-mêmes reconnaissent que, dans le tumulte du début, bien des décisions étaient davantage fondées sur l'intuition et l'expérience que sur la planification ou la politique. Il n'est donc guère surprenant que de telles décisions aient parfois semblé arbitraires et aient donné prise à des rumeurs de discrimination et de favoritisme.

Un autre facteur était la nostalgie de la GRC. Les gestionnaires qui ont appris leur métier dans la hiérarchie rigide de la GRC s'attendaient à une obéissance rapide et silencieuse, et non à la remise en question de leurs décisions.

Pour terminer, il y a la valeur attachée au principe du besoin de savoir dans toute agence de sécurité et de renseignements. Ce principe est, évidemment, essentiel aux questions de sécurité. Mais il ne doit pas déborder sur les pratiques administratives. Le SCRS n'a pas fait connaître, par exemple, sa politique régissant les mutations.

Guide du personnel. Comme dans le domaine des langues officielles, le SCRS prenait des mesures pour résoudre ses problèmes en matière de relations de travail. Nous avons été particulièrement soulagés d'apprendre qu'il rédigeait un guide officiel d'administration du personnel. En clarifiant les règles, ce guide peut prévenir beaucoup de malentendus et de méfiance.

Le SCRS propose également que la Commission des relations de travail dans la Fonction publique (CRTFP) soit habilitée à régler les griefs présentés par des employés non syndiqués comme les agents de renseignements, les surveillants et les analystes. À l'heure actuelle, le directeur est l'arbitre ultime de ces griefs, ce qui le met dans la position gênante d'être à la fois juge et partie.

Notre seul souci est de nous assurer que la modification recherchée de la *Loi sur les relations de travail dans la Fonction publique* confère effectivement à la CRTFP un mandat suffisant pour entendre les griefs du SCRS.

Conversion. Une des controverses majeures à l'origine de notre enquête concernait la «conversion», c'est-à-dire l'occasion qui a été donnée aux surveillants (les anciens «agents spéciaux» de la GRC, les personnes qui filent les cibles) de se porter candidats à des postes d'agents de renseignements (AR).

C'était là une occasion rêvée pour les surveillants. Leurs postes étaient sans issue; une surveillance diligente et habile était récompensée par la chance de faire plus de surveillance. Un AR, d'autre part, constitue le premier échelon à gravir pour accéder au poste de directeur.

Les problèmes de communications ont malheureusement tourné la conversion en champ de bataille. En premier lieu, les surveillants interrogés pendant notre enquête croyaient que la distinction entre eux-mêmes et les AR serait complètement effacée : le cheminement de carrière serait le même pour tous. Au moins certains surveillants à Montréal croyaient que leur candidature aux postes d'AR aurait priorité absolue sur celle de toute personne de l'extérieur.

Ces deux espoirs étaient vains. La direction du SCRS interprète ses promesses en termes beaucoup plus étroits. Elle croit les avoir tenues en permettant aux surveillants de se porter candidats aux postes d'AR sans détenir de diplômes universitaires (ce qu'ont peu de surveillants) ni avoir suivi la formation de base à l'Académie Sir William Stephenson.

Entente de permutation. Les surveillants à Montréal croyaient aussi qu'une entente de permutation qui leur avait été présentée comme une condition de conversion était une tentative pour leur faire peur. Cette entente soulevait la possibilité d'une mutation, et l'on sait depuis belle lurette que les Montréalais francophones dans tous les domaines préfèrent faire carrière à Montréal. Les surveillants ne faisaient pas exception à cette règle.

Grave entorse à la pratique établie en matière de langues officielles, le SCRS a d'abord offert les tests psychologiques en anglais seulement, puis il a obligé ceux qui insistaient sur des tests en français à attendre six mois. C'est seulement le «fossé culturel» que nous avons mentionné sous la rubrique des langues officielles ci-dessus qui peut expliquer ce traite-

ment inégal des candidats francophones et anglophones à la conversion et ce défaut d'anticiper la réaction.

Ensuite, un deuxième concours de conversion a été annoncé avant la fin du premier à Montréal. Les surveillants à Montréal n'avaient apparemment pas été informés que le premier concours était terminé dans le reste du pays, et ils en ont vite conclu—ce qui est compréhensible quoique, pour autant que nous sachions, faux—qu'on voulait leur jouer par là un mauvais tour.

Autres problèmes. Nos constatations concernant la procédure applicable aux griefs sont évidentes d'après ce que nous avons déjà dit et d'après les recommandations formulées plus bas.

Nous avons également déterminé que la perspective de mutations latérales mal expliquées insécurisait gravement les employés, et qu'ils croyaient généralement que les concours d'avancement dissimulaient le favoritisme sans le prévenir, et que les employés du SCRS (qui ne sont pas, légalement parlant, des fonctionnaires) se sentent pris au piège parce qu'ils ne sont pas admissibles aux concours internes de la Fonction publique.

Recommandations. Voici nos principales recommandations concernant les relations de travail :

- Que la *Loi sur les relations de travail dans la Fonction publique* soit modifiée de façon à ce que les griefs des employés non syndiqués du SCRS puissent être entendus par un membre de la Commission des relations de travail dans la Fonction publique détenant l'habilitation de sécurité requise.
- Que les employés non syndiqués, qui ne sont pas assujettis à une convention collective, soient autorisés à présenter des griefs fondés sur le Guide d'administration du personnel.
- Que la réponse du directeur à un grief donne toujours les motifs de décision.
- Que des arrangements visant les déductions à la source soient pris afin de fournir à l'Association des employés du SCRS des fonds pour payer les frais d'arbitrage si l'Association décide de jouer un rôle dans de telles procédures, et que le montant des déductions soit déterminé par un vote majoritaire des membres de l'Association.
- Que le SCRS fasse une déclaration de principe décrivant les cheminements de carrière accessibles à ses employés, surtout ceux qui ne font pas partie de la catégorie des AR, et énonçant les règles qui régissent la conversion d'un cheminement à l'autre.
- Que le SCRS fasse une déclaration de principe précisant les conditions des mutations latérales.
- Que les jurys de sélection du personnel se composent du superviseur du futur titulaire, d'un superviseur de niveau équivalent provenant d'une autre direction du Service et d'un agent de la Commission de la Fonction publique qui détient l'habilitation de sécurité requise.
- Que le SCRS examine des façons de permettre à ses employés de postuler des emplois dans la Fonction publique.

9. Plaintes

Les plaintes touchant à la citoyenneté et à l'immigration ont constitué la majeure partie de notre travail en 1986-1987.

Leur importance n'était pas seulement quantitative. Elles sont plus complexes et difficiles que les causes d'habilitations de sécurité et elles comportent habituellement un grand nombre de rapports et de documents accumulés pendant nombre d'années. Et les enjeux sont de taille. Un rapport défavorable de notre part pourrait très bien amener le gouverneur en conseil à refuser la citoyenneté ou à ordonner que des procédures de déportation soient amorcées.

Entre-temps, le nombre de nouvelles plaintes concernant les habilitations de sécurité a dégringolé.

Un bon point pour la défense

Les nouvelles procédures de filtrage du ministère de la Défense nationale (MDN) semblent compter pour beaucoup dans la baisse des plaintes visant les habilitations de sécurité.

Dans notre dernier rapport annuel, nous nous sommes formellement opposés à la façon dont le MDN effectuait ses enquêtes visant les habilitations de sécurité.

Nous sommes heureux cette année de répéter publiquement ce que nous avons déjà dit en privé, c'est-à-dire que le MDN a fait preuve d'un véritable respect pour la dignité individuelle en révisant radicalement ses procédures relatives aux habilitations de sécurité.

Une habilitation de sécurité a été accordée dans au moins 39 des 44 affaires que nous avons demandé au MDN de reconsidérer en 1986. Les cinq autres personnes ont retiré leurs plaintes sur l'assurance que leur cas serait revu à une date ultérieure.

Aucune nouvelle plainte n'a été portée contre le MDN en 1986-1987. Nous espérons que le Ministère continuera de respecter la norme élevée qu'il a établie pour lui-même. Par prudence, nous avons demandé au MDN de nous informer annuellement du nombre d'habilitations de sécurité qu'il a refusées. Si les refus sont nombreux, mais que les plaintes sont rares, nous demanderons des précisions.

Habilitations de sécurité

Le nombre de nouvelles plaintes concernant des habilitations de sécurité refusées par d'autres ministères a également chuté; il n'y en a eu qu'une en 1986-1987, comparativement à 14 l'année précédente.

Nous aimons à penser que cela est dû aux plus grands soins qui sont pris à mesure que les responsables de la sécurité—dans les ministères et organismes aussi bien qu'au SCRS—se familiarisent avec le processus applicable aux plaintes et avec les critères qui se précisent chaque fois que nous traitons des cas particuliers.

En 1986, le gouvernement a mis sur pied un nouveau système de classification et de filtrage de sécurité. Ce système n'entre pas directement dans nos attributions relatives au

contrôle. Mais, comme il constitue un élément important des plaintes que nous entendons ainsi que de la charge de travail du SCRS, nous en reparlons plus loin dans le présent chapitre.

Mandats. En vertu de la *Loi sur le SCRS* (article 42), les personnes qui suivent peuvent nous présenter des plaintes :

- Une personne qui se voit refuser un emploi au gouvernement fédéral pour la seule raison du refus d'une habilitation de sécurité.
- Un employé fédéral qui fait l'objet d'une décision de renvoi, de rétrogradation, de mutation ou d'opposition à avancement ou mutation pour la même raison.
- Toute personne qui fait l'objet d'une décision d'opposition à un contrat de fourniture de biens ou de services au gouvernement pour la même raison.

Le ministère de la Défense nationale effectue son propre filtrage de sécurité*. Dans les autres ministères et organismes, la décision d'accorder ou de refuser une habilitation est prise par l'administrateur général après soumission d'une évaluation de sécurité par le SCRS.

Quiconque se voit nier une habilitation de sécurité doit être averti et informé qu'il peut nous présenter une plainte officielle. Après une enquête et la tenue d'audiences à *huis clos* par au moins un membre de notre Comité, nous faisons rapport de nos conclusions et recommandations, s'il y en a, au solliciteur général, au directeur du SCRS, à l'administrateur général concerné et au plaignant.

Enquêtes et recommandations. Cette année, des audiences ont été tenues et des recommandations formulées dans deux cas. Dans le premier, nous avons recommandé qu'une habilitation soit accordée, ce qui a été fait. Dans le second, nous avons appuyé la recommandation du SCRS qui s'était prononcé contre l'habilitation. Des résumés de ces causes se trouvent à l'Annexe B. Une plainte du même genre était toujours à l'étude à la fin de l'année.

Plaintes contre le SCRS

Mandat. La *Loi sur le SCRS* exige que nous fassions enquête sur les plaintes concernant «des activités du Service» (article 41).

Il y a deux conditions principales. Primo, la plainte doit être présentée au directeur du SCRS. Nous pouvons l'accepter si le directeur n'a pas répondu dans un délai que nous jugeons normal ou si le plaignant n'est pas satisfait de sa réponse.

Secundo, nous ne pouvons enquêter sur une plainte susceptible d'être réglée par une autre procédure de griefs prévue dans la *Loi sur le SCRS* ou la *Loi sur les relations de travail dans la Fonction publique*.

* La GRC également.

Plaintes des employés. Le commissaire aux langues officielles et nous-mêmes avons reçu 1 776 plaintes en 1986-1987 au sujet des pratiques en matière de langues officielles du Service, soit environ trois fois plus que l'an passé. Ces plaintes ont toutes été portées par des employés du SCRS.

Nous les avons tenues en suspens pendant que le Bureau du commissaire faisait une vérification détaillée du bilinguisme officiel dans le Service, et pendant que nous menions l'enquête examinée au chapitre 8.

Plaintes du public. Nous avons reçu 13 plaintes de membres du public, par opposition à quatre l'année précédente. Douze, provenant surtout de personnes dont la candidature à un poste au sein du SCRS avait été rejetée, outrepassaient nos compétences et une était à l'étude à la fin de l'année.

Immigration et citoyenneté

Nous avions 13 cas de citoyenneté et un cas d'immigration devant nous au début de 1986-1987. Nous avons été saisis de cinq nouvelles causes d'immigration pendant l'année, mais d'aucune nouvelle cause de citoyenneté*.

Mandats. En vertu de la *Loi sur la citoyenneté*, le secrétaire d'État nous fait rapport lorsqu'il est d'avis que la citoyenneté devrait être refusée à un particulier parce qu'il existe des motifs raisonnables de penser que celui-ci constitue une menace envers la sécurité du Canada ou est impliqué dans le crime organisé.

De même, en vertu de la *Loi sur l'immigration de 1976*, un rapport nous est communiqué lorsque le ministre de l'Emploi et de l'Immigration et le solliciteur général croient qu'une personne demandant son admission au Canada participera, de diverses façons précises, à des activités qui sont contraires aux intérêts du Canada.

Dans les deux cas, la personne faisant objet du rapport doit être avisée. Nous enquêtons comme nous le ferions en regard d'une plainte du particulier, et nous faisons des recommandations au gouverneur en conseil.

Enquêtes et recommandations. Une cause d'immigration a été tranchée, et nous avons convenu que l'admission au Canada devrait être refusée. Les enquêtes se poursuivent dans quatre cas d'immigration et un cinquième cas a été rouvert avec l'accord de toutes les parties.

Six causes de citoyenneté ont été réglées. Dans deux, nous avons recommandé que la citoyenneté soit accordée. Une cause de citoyenneté a pris fin avec le décès du requérant. En outre, le SCRS a retiré ses objections pendant l'enquête dans trois cas de citoyenneté.

---

* Les lecteurs qui aiment l'analyse statistique voudront peut-être savoir que: a) une des causes d'immigration et une des causes de citoyenneté portent sur la même personne et que b) une des nouvelles causes d'immigration est identique à l'une des causes reportées de l'année précédente; elle a été rouverte avec le consentement de toutes les parties.

Des résumés de causes touchant à la citoyenneté et à l'immigration se trouvent également à l'Annexe B.

Un rapport sur un cas de citoyenneté était en voie de rédaction à la fin de l'année, et les enquêtes se poursuivaient dans six cas.

La première cause concernant les dispositions sur la criminalité de la *Loi sur l'immigration de 1976* nous est parvenue à la fin de l'année. Nous avions des raisons d'en attendre davantage au début de 1987-1988.

Qualité des enquêtes

Nous avons déjà mentionné l'amélioration marquée dans la qualité des enquêtes menées par le ministère de la Défense nationale.

Évaluations de sécurité du SCRS. Au cours des trois dernières années, nous avons vu de nombreux rapports sur le filtrage de sécurité rédigés par le SCRS pour le compte d'autres ministères et organismes et, pour la plupart, ils étaient bien faits.

Cependant, dans les cas que nous avons vus cette année, des conclusions ont été tirées de preuves insuffisantes et des activités qui auraient pu être parfaitement innocentes ont parfois été présentées, sans raison valable, sous le pire jour possible. Les rapports sur ces causes mettaient ces lacunes en lumière.

Immigration et citoyenneté. Nous avons été particulièrement déçus par la qualité des rapports du SCRS et des preuves qu'il nous a fournies dans les causes de citoyenneté et d'immigration.

Par exemple, le Service mettait parfois des semaines à répondre à des questions simples que nous lui avions posées pendant l'enquête préliminaire, et il arrivait parfois aux audiences en possession de preuves que n'avaient pas vues les ministres à qui la recommandation initiale avait été faite.

Ni les délais ni l'accumulation ultérieure de preuves ne révèlent sous un éclairage favorable l'attention que requièrent des recommandations dont peut dépendre le reste d'une vie d'un individu.

Rapport spécial. Nous avons présenté un rapport spécial au solliciteur général, en vertu de l'article 54 de la *Loi sur le SCRS*, afin de lui faire connaître nos préoccupations concernant à la fois les évaluations de sécurité et le traitement des causes de citoyenneté et d'immigration par le SCRS.

Un rapport spécial s'imposait parce que le SCRS n'accepte pas nos préoccupations. En fait, il semble blâmer le processus exigé par la *Loi sur le SCRS*—ou notre interprétation de celui-ci.

Pour améliorer les contrôles, nous avons recommandé ce qui suit :

- Que le directeur (ou, en son absence, un sous-directeur) du SCRS détienne personnellement le pouvoir exclusif de recommander que, pour des raisons de sécurité, la citoyenneté soit niée, l'entrée soit refusée à un immigrant ou à un visiteur éventuel, ou un résidant permanent soit déporté.
- Que ces recommandations soient présentées au solliciteur général qui, s'il les accepte, autorisera alors la transmission du rapport au secrétaire d'État dans les causes de citoyenneté ou, dans les causes d'immigration, transmettra le rapport lui-même, accompagné de ses propres commentaires, au ministre de l'Emploi et de l'Immigration.
- Que, de même, le commissaire de la GRC (ou, en son absence, le sous-commissaire) détienne personnellement le pouvoir exclusif de présenter des recommandations au solliciteur général concernant la déportation en vertu des dispositions sur la criminalité de la *Loi sur l'immigration de 1976*.
- Que le directeur du SCRS (ou, en son absence, un sous-directeur) détienne le pouvoir exclusif de recommander qu'une habilitation de sécurité soit refusée à un Canadien postulant un emploi au gouvernement fédéral.

Nous espérons discuter de cette question en détail avec le SCRS le plus tôt possible et pouvoir déclarer l'an prochain que des procédures plus efficaces ont été élaborées en vue de maintenir l'équilibre délicat qui existe entre la protection de la sécurité du Canada et la protection des droits individuels.

Étude concernant la Loi sur l'immigration

Dans un rapport le 17 juin 1986, le Comité permanent de la Chambre des communes chargé du travail, de l'emploi et de l'immigration a fait deux recommandations concernant le filtrage de sécurité, à savoir :

> 32. Que le solliciteur général demande au Comité de surveillance des activités de renseignement de sécurité d'enquêter et de présenter un rapport sur la question de savoir si la *Loi sur l'immigration du Canada* protège adéquatement le Canada, et que tout changement législatif recommandé soit présenté au Parlement aussitôt que possible.
>
> 34. Que le solliciteur général demande au Comité de surveillance des activités de renseignement de sécurité de revoir les dispositions sur la criminalité de la *Loi sur l'immigration*.

Le 26 septembre 1986, le solliciteur général nous a officiellement demandé d'enquêter et de faire un rapport sur l'efficacité des dispositions pertinentes de la *Loi sur le SCRS*. En vertu de l'article 40 de cette loi, nous avons demandé à l'inspecteur général de recueillir des renseignements pour nous. Notre travail à cet égard se poursuivait à la fin de l'année.

Nous avons également été invités à faire partie du groupe de travail interministériel formé par le ministre d'État (Immigration) et chargé d'élaborer la réaction du gouvernement au rapport du Comité permanent. Nous sommes représentés par le secrétaire exécutif.

Nous ne jouons un rôle exécutif dans ni l'une ni l'autre de ces activités. Mais notre expérience des affaires d'immigration et des affaires de citoyenneté lesquelles sont presque identiques nous a donné une perspective unique que nous estimons devoir mettre à la disposition du Gouvernement lorsqu'il étudiera les modifications de la *Loi sur l'immigration de 1976*.

Nous croyons que ces mesures seront préventives. Mieux vaut offrir nos conseils dès maintenant dans l'espoir de prévenir les problèmes que de grogner dans les coulisses lorsque des problèmes surgiront.

La nouvelle politique de sécurité

Le 18 juin 1986, le solliciteur général d'alors a élaboré une nouvelle politique en matière de sécurité et de nouvelles lignes directrices opérationnelles régissant la classification de l'information et le filtrage du personnel.

La politique préalable provenait d'un document du BCP daté de 1956 et appelé Security of Information in the Public Service of Canada. Il était complété par le Document du Cabinet (Doc. du Cab.) 35 qui remonte à 1963. Il est de commune renommé que trop d'information était classifiée et que des habilitations de sécurité étaient demandées pour trop de personnes en vertu de ces arrangements.

Les coûts sont un facteur qui limite la portée de la politique visant la sécurité. Une habilitation de sécurité coûterait en moyenne 1 425 $ au niveau très secret, et 13,62 $ aux niveaux confidentiel et secret—chiffres qui, selon nous, sont gravement sous-évalués, comme nous l'avons expliqué dans notre rapport annuel de l'an dernier.

La réforme visait également à accélérer le processus de filtrage des particuliers en réduisant la demande. À l'époque, le SCRS était submergé d'enquêtes de sécurité à effectuer, et ces arrérages dans le travail allaient en s'accroissant. Nous avons également décrit cette situation dans notre rapport annuel de l'an dernier.

Demande. Les nouvelles mesures devaient réduire la demande des habilitations de sécurité en exigeant que les requêtes soient justifiables, équitables et effectives. Les objectifs suivants ont été établis :

- Seulement l'information dont la protection contre la divulgation non autorisée est essentielle à l'intérêt national doit être classifiée.
- Les ministères et organismes doivent réduire le nombre de postes exigeant une habilitation de sécurité.
- Les droits des particuliers touchés par le système de sécurité administratif du gouvernement doivent être améliorés.
- La sécurité du Canada doit être accrue grâce à une gestion plus efficace des ressources consacrées aux programmes de filtrage de sécurité ainsi que de classification et de protection de l'information.

Aux termes de la nouvelle politique, l'information doit être classifiée seulement si elle s'inscrit dans l'une des six catégories suivantes : la défense nationale, les affaires internationales, la sécurité nationale (y compris les activités hostiles et subversives et les menaces envers la sécurité du Canada), les documents confidentiels du Cabinet, les affaires fédérales-provinciales, et certains intérêts économiques du Canada.

Les administrateurs généraux sont responsables de la sécurité dans leurs ministères et organismes. Entre autres choses, ils déterminent quels employés doivent obtenir une habilitation de sécurité et s'assurent que ces derniers sont filtrés avant d'entrer en fonction.

Sauf, comme nous l'expliquons ci-dessus, dans le cas du MDN et de la GRC, une «évaluation de sécurité» est fournie par le SCRS. Mais la décision ultime d'accorder ou de refuser une habilitation incombe à l'administrateur général.

Critères de rejet. En vertu de la nouvelle politique, une habilitation de sécurité ne peut être refusée pour cause de déloyauté à moins qu'il n'existe des motifs raisonnables de penser que la personne en question se livre ou pourrait se livrer à des activités qui correspondent à la définition de «menaces envers la sécurité du Canada» figurant dans la *Loi sur le SCRS* (article 2).

Le Doc. du Cab. 35 prévoit qu'une personne peut être rejetée parce qu'elle n'est «pas fiable», et pas simplement parce qu'elle est carrément déloyale. C'est encore le cas, mais il doit exister des motifs raisonnables de penser que ce particulier pourrait divulguer des informations classifiées (par des propos inconsidérés, par exemple), ou pourrait être incité à en divulguer (par des menaces de chantage, par exemple), ou encore pourrait être la cause de la divulgation de telles informations (par sa négligence habituelle).

Le Conseil du Trésor, qui est responsable de la gestion globale des nouvelles politiques, aide chaque ministère à mettre en oeuvre le programme et s'assure qu'il est conforme à la nouvelle politique.

Le 12 septembre 1986, le solliciteur général a donné au SCRS une directive officielle régissant la prestation des évaluations de sécurité.

Redressement. Lors de l'annonce de la nouvelle politique en matière de sécurité, le solliciteur général de l'époque a réaffirmé que le gouvernement s'était engagé à établir une procédure de révision juste et équitable pour les personnes qui s'étaient vu refuser une habilitation de sécurité. Il s'est exprimé ainsi :

> Le Comité de surveillance des activités de renseignement de sécurité se compose de cinq membres du Conseil privé représentant les trois partis politiques à la Chambre des communes. À titre d'organisme autonome, le Comité a pour mandat d'examiner les plaintes concernant les habilitations de sécurité exigées par le gouvernement, et il a pleins pouvoirs pour exiger la production de preuves et de témoins par le Service et par le ministère qui a refusé l'habilitation de sécurité.
>
> Le SCRS a démontré son utilité à titre de mécanisme de révision, grâce au soin, à la minutie et à l'équité avec lesquels il a fait enquête sur les cas qui lui ont été soumis

jusqu'ici et sur lesquels il a fait rapport. Dans chaque cas, le Service a su faire valoir les principes de justice naturelle qui étaient en jeu.*

Incidence sur le SCRS. Nous n'avons pas étudié en profondeur l'incidence de la nouvelle politique en matière de sécurité sur le SCRS. Toutefois, nous avons noté les trois éléments suivants qui ajouteront à sa charge de travail, à savoir :

- Le SCRS établira et tiendra un fichier central de toutes les demandes touchant les habilitations de sécurité.
- En ce qui concerne le filtrage de sécurité nécessitant des vérifications aux casiers judiciaires et des vérifications de crédit, le Service sera le seul point de contact de tous les ministères sauf le MDN et la GRC.
- En tant que projet pilote, des entrevues personnelles seront tenues avec les personnes devant être habilitées au niveau secret, alors qu'elles étaient préalablement requises pour un motif valable seulement. Des entrevues personnelles sont maintenant obligatoires pour l'habilitation au niveau très secret.

Aucune diminution. Six mois après l'annonce de la nouvelle politique, notre recherche n'indiquait aucune diminution dans les demandes d'évaluations de sécurité. En fait, si les demandes d'enquêtes sur le terrain—correspondant plus ou moins aux demandes d'habilitation au niveau très secret—étaient à la baisse, l'ensemble des chiffres a augmenté après la mise en oeuvre de la nouvelle politique. Le Tableau 6 renferme les chiffres pour les six derniers mois de 1985 et de 1986.

Tableau 6. Demandes d'évaluations de sécurité

	demandes d'habilitations de sécurité	demandes d'enquêtes sur le terrain
deuxième semestre, 1985	31 797	2 005
deuxième semestre, 1986	35 061	1 425

(Source : SCRS)

Ces chiffres comprennent les habilitations aux trois niveaux, à savoir confidentiel, secret et très secret.

Le solliciteur général a pris un certain nombre de mesures pour remédier à cette situation.

Sur un plan pratique, il a ordonné à la Direction du filtrage de sécurité du SCRS d'obtenir l'aide de secrétariat temporaire dont elle avait besoin pour éliminer le retard qui existait dans environ mille cas dont l'enquête était terminée mais qui s'accumulaient en attendant d'être dactylographiés.

* *Débats de la Chambre des communes*, 18 juin 1986.

En décembre 1986 il a aussi demandé au Service de renvoyer dans les différents ministères les cas qu'il n'avait pas encore tranchés pour qu'ils les reconsidèrent à la lumière de la nouvelle politique.

Enfin, il a demandé au coordonnateur, Renseignements et Sécurité, du Bureau du Conseil privé de s'entretenir personnellement avec les administrateurs généraux des ministères qui demandent des habilitations au niveau très secret non justifiées aux termes de la nouvelle politique.

10. Précisions diverses

Notre travail dans le secteur du contrôle et de l'enquête des plaintes n'est pas un mystère pour les lecteurs des chapitres précédents. Mais certaines de nos activités ne correspondent à ni l'une ni l'autre de ces rubriques. Nous les décrivons ci-dessous.

Comptes rendus au Parlement

En 1986, nous avons comparu à deux reprises devant le Comité permanent de la Chambre des communes chargé de la justice et du solliciteur général, à savoir le 3 juin pour répondre à des questions sur notre rapport annuel de 1984-1985 et le 20 novembre pour répondre à des questions sur notre rapport annuel de 1985-1986. Les questions qui nous ont été posées à ces moments-là sont traitées dans le présent rapport.

À la fin de l'année à l'étude, nous étions censés comparaître le 3 avril 1987 devant le Comité sénatorial spécial du terrorisme et de la sécurité publique.

Sensibilisation

En rendant compte au Parlement, nous nous estimons responsables vis-à-vis les Canadiens dans l'ensemble du pays.

En accord avec le fait qu'il nous revient d'informer et de sensibiliser le public dans les secteurs de la sécurité et du renseignement, nous sommes aussi ouverts que la sécurité nous permet de l'être auprès des centaines de particuliers qui nous posent des questions au sujet des procédures applicables aux habilitations de sécurité et d'incidents particuliers ou de points généraux.

Mass médias. Nous sommes également aussi sincères que possible avec les mass médias. Après avoir présenté notre deuxième rapport annuel au Parlement en juin 1986, nous avons tenu une conférence de presse et notre président, l'honorable Ronald G. Atkey, ainsi que d'autres membres et employés ont été interviewés nombre de fois pendant l'année. Nous croyons que, dans une démocratie saine, il peut et devrait y avoir une certaine discussion publique réfléchie sur des questions touchant à la sécurité.

Il arrive aussi que nous puissions rendre des questions publiques au nom du SCRS, lorsqu'il ne peut le faire lui-même. Nous pouvons alors mettre les questions en perspective au profit de toutes les personnes concernées.

Réunions et conférences

Le président et le personnel sont également interviewés par les recherchistes et les étudiants des universités. Nous restons en contact avec les spécialistes universitaires et professionnels du renseignement de sécurité, pas seulement parce que nous nous estimons tenus de partager largement nos propres constatations, mais pour ce qu'ils peuvent nous enseigner.

L'an passé, le président :

- A participé au Forum national sur l'accès à l'information et la protection des renseignements personnels offert par le ministère de la Justice et le Conseil du Trésor le 7 mars 1986.
- A présenté un document intitulé «The Security Intelligence Review Committee : Legislative Oversight and Government Policy in Canada Today» à une conférence sur le renseignement et la politique parrainée par le Defence Intelligence College à Washington (D.C.) des 26 au 28 août 1986.
- A traité de «l'obligation de rendre compte du Comité du renseignement de sécurité» à un séminaire organisé par les professeurs Clifford Shearing et Stewart Farson au Centre of Criminology à l'Université de Toronto, le 24 février 1987.
- A prononcé une allocution devant les étudiants de la Osgoode Hall Law School de l'Université York inscrits à un cours sur la sécurité et le renseignement, le 11 mars 1987, et a participé à la discussion qui a suivi. La session était organisée par Peter Hanks, professeur invité d'Australie.

Deux membres, l'honorable Jean Jacques Blais et l'honorable Frank McGee, ont assisté à la National Conference on Law in Relationship to Terrorism, parrainée par la American Bar Association à Washington (D.C.) des 5 au 7 juin 1986.

Notre secrétaire exécutif et un agent de recherche ont participé à une conférence sur la psychologie du terrorisme qui a eu lieu à Washington (D.C.) au Woodrow Wilson Center, International Security Studies Program, les 16 et 17 mars 1987.

En plus d'avoir assisté avec le président à la conférence des 26 au 28 août 1986 sur le renseignement et la politique parrainée par le Defence Intelligence College à Washington (D.C.), le directeur de la recherche a assisté à la deuxième conférence annuelle de la Canadian Association of Security and Intelligence Studies à l'Université du Manitoba à Winnipeg le 7 juin 1986.

L'adjointe exécutive et l'agent principal chargé des plaintes ont eu deux rencontres avec les fonctionnaires du U.S. Defence Department pour étudier la politique en matière de sécurité du personnel et pour échanger des idées—d'abord au Pentagon le 14 novembre 1986, puis au Personnel Security Research and Education Center à Monterey (Californie) les 15 et 16 janvier 1987. Au Research and Education Center, l'adjointe exécutive a présenté un exposé sur l'évolution du processus de filtrage de sécurité au gouvernement du Canada.

Un agent de recherche a assisté à un symposium sur les stratégies actuelles et futures visant les tests d'aptitudes professionnelles tenu le 21 juin 1986, organisé dans le cadre de la conférence annuelle de la Société canadienne de psychologie.

Personnel

Notre bureau n'a pas grossi depuis la fin de l'an dernier; pendant toute la durée de 1986-1987, nous n'avions toujours que 13 employés, malgré une charge de travail à la hausse.

Ces employés relèvent d'un secrétaire exécutif qui dirige toutes les opérations quotidiennes. Nos autres employés comprennent un directeur de la recherche, deux recherchistes et une adjointe de recherche, un agent principal chargé des plaintes, une adjointe exécutive qui remplit des fonctions relatives à la recherche et aux plaintes, un agent administratif qui est également le greffier de nos audiences et le coordonnateur des requêtes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, ainsi que cinq employés de soutien. Une liste complète de nos employés et de leur numéro de téléphone se trouve à l'Annexe C.

Rapport financier

Notre budget pour 1986-1987 est exposé au Tableau 7. Nous avions d'abord affecté 344 000 $ aux dépenses de biens et services en 1986-1987, mais nous avons été obligés de quasiment doubler cette somme en présentant des budgets supplémentaires, afin de satisfaire des besoins qui ne pouvaient pas être prévus lorsque le budget principal a été dressé en 1985, notamment :

- Effectuer, à la demande du solliciteur général, une étude spéciale des problèmes posés par les langues officielles et les relations de travail au SCRS (voir la page 57, chapitre 8 du présent rapport).
- Payer les frais judiciaires occasionnés par le processus applicable aux plaintes.

Tableau 7. Budget du CSARS, 1986-1987

Personnel		545 000 $
Traitements et salaires	75 000 $	
Contributions aux régimes d'avantages sociaux des employés	70 000 $	
Biens et services		677 000 $
Services professionnels	519 000 $	
Autres	158 000 $	
Total des dépenses de fonctionnement		1 222 000 $
Capital		9 000 $
Total des dépenses		1 231 000 $

(Source : Budget des dépenses pour 1986-1987, Partie III)

11. Projets d'avenir

Nos priorités pour 1987-1988 comprennent le programme d'antiterrorisme du SCRS, son processus d'analyse et de production des renseignements et la protection des secrets scientifiques et techniques.

Notre travail relatif à la protection des secrets scientifiques et techniques a déjà commencé, et nous pouvons en toucher un mot ici, de manière à en donner le ton.

Science et Technologie. Les secrets militaires traditionnels ne sont plus les seules cibles de l'espionnage. Les connaissances scientifiques et techniques doivent aussi être protégées. En tant que membre de la communauté scientifique ainsi que des alliances militaires occidentales, le Canada a le devoir de sauvegarder la science et la technologie empruntées aussi bien que celles qu'il a lui-même développées.

Nous étudions un certain nombre de questions qui découlent de ces considérations, c'est-à-dire :

- La participation du SCRS à l'élaboration de politiques destinées à protéger nos avoirs scientifiques et techniques et ceux de nos alliés.
- Les renseignements que le SCRS fournit aux ministères fédéraux s'occupant du contrôle des exportations et d'autres mesures destinées à protéger les connaissances secrètes d'ordre scientifique et technique.
- La priorité accordée par le SCRS à la collecte de renseignements concernant les vols de science et de technologie et les ressources qu'il consacre à cette tâche.
- La question de savoir si l'identification des cibles éventuelles par le gouvernement est adéquate.
- Les dispositions qui sont prises pour le filtrage de sécurité des employés travaillant dans les établissements de haute technologie qui ont accès à des connaissances secrètes d'ordre scientifique et technique.

Le SCRS nous a donné des séances d'information sur ces questions et nous poursuivons notre enquête.

Examen quinquennal

Toutefois, notre préoccupation primordiale pendant l'année à venir sera de dresser une liste complète des questions que le Parlement pourra vouloir aborder lorsqu'il effectuera l'examen quinquennal de la *Loi sur le SCRS* en 1989.

Nous avons l'intention de consulter les particuliers intéressés, les groupes d'intérêt pertinents et des experts au sein des universités, du gouvernement et ailleurs. Cela nous permettra de mettre à l'essai les conclusions que nous avons tirées de notre expérience et donnera à ces parties l'occasion de nous faire profiter à l'avance de leurs intuitions.

Le présent rapport est parsemé de questions qui sont surgies d'elles-mêmes pendant nos activités d'examen courantes—par exemple, la protection des relations privilégiées entre un avocat et son client (page 22) et la valeur des statistiques de base sur les mandats judiciaires (page 13).

La portée du contrôle

La fonction de contrôle elle-même est une autre question qui pointe déjà à l'horizon. La *Loi sur le SCRS* a établi un précédent en créant le présent comité pour surveiller le Service. Mais le secteur canadien de la sécurité et du renseignement comporte d'autres intervenants importants, qui ne sont inclus dans aucun contrôle indépendant.

Annuaire des agences canadiennes de sécurité et de renseignement. En fait, lorsque nous avons assumé nos fonctions en 1984, nous avons été surpris de ne pas même pouvoir trouver un annuaire complet des organismes du gouvernement fédéral travaillant dans le secteur de la sécurité et du renseignement.

Nous estimions qu'il était important pour nous de connaître les agences soeurs du SCRS. Dans un premier temps, nous serions davantage en mesure de comprendre le mandat du SCRS si nous connaissions les mandats des autres agences et les rapports du SCRS avec elles. Nous étions particulièrement intéressés par les comités qui diffusent des informations sur la sécurité et le renseignement et qui fondent leurs décisions sur ces informations. Connaître les besoins de pareils comités améliorerait notre compréhension des objectifs opérationnels du SCRS et de ses rapports, réels et potentiels.

Incapables de trouver un annuaire complet, nous avons décidé d'en faire un nous-mêmes, tâche que nous avons terminée en 1986-1987.

Nous reconnaissons, avec regret, que nous ne pouvons pas rendre cet annuaire public. Il contient des informations—notamment des descriptions des rôles joués par certaines agences—qui seraient beaucoup trop intéressantes pour les ennemis de notre pays. Nous avons également promis d'en limiter la diffusion afin d'obtenir la collaboration de certaines agences qui n'étaient pas légalement tenues de nous fournir des informations.

Cependant, nous en avons mis des copies à la disposition du secteur canadien de la sécurité et des renseignements lui-même et nous avons été heureux des réactions fort favorables qu'elles ont suscitées. Il semble que nous n'étions pas les seuls à penser qu'il est utile de savoir qui au juste fait quoi.

Ces réactions nous ont convaincus de réviser et de distribuer les annuaires annuellement, aussi bien pour nous tenir au courant que pour mieux servir le secteur de la sécurité et du renseignement au Canada.

Documents confidentiels du Cabinet. Le fait que nous n'avons pas accès aux documents confidentiels du Cabinet apporte une autre limite à nos pouvoirs actuels. Nous n'avons pas considéré cette limite comme sévère jusqu'à présent, mais, évidemment, nous ne pouvons pas vraiment savoir de ce qu'il nous manque. Cette lacune pourrait devenir un problème si un Cabinet se mettait à apposer le sceau de la confidentialité sur un trop grand nombre de renseignements.

Nous notons que le comité de la Chambre des communes chargé de la justice et du solliciteur général a recommandé de resserrer la définition des documents confidentiels du Cabinet aux fins de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des rensei-*

*gnements personnels**, et nous attendons la réaction du gouvernement avant d'adopter une position plus précise.

Un dernier mot

Maintenant que notre mandat quinquennal est à demi terminé, c'est avec assez de satisfaction que nous pensons à tout ce que nous avons pu accomplir, et non sans appréhension que nous songeons à tout ce qu'il nous reste à faire.

Pourtant, en réfléchissant à notre travail jusqu'à présent, nous continuons d'apprécier deux aspects importants de notre mandat. Le premier est notre nomination à titre de membres à temps partiel, actifs dans d'autres secteurs de la collectivité et dans la vie privée. Nous avons pu, de ce fait, rester un peu plus objectifs et détachés des intrigues quotidiennes du renseignement de sécurité en particulier et des affaires gouvernementales en général. Nous espérons que cela a aiguisé nos aptitudes analytiques et notre jugement.

Deuxièmement, nous avons eu la bonne fortune de pouvoir attirer des professionnels compétents et travailleurs en tant que membres de notre effectif permanent ainsi que des consultants et avocats de l'extérieur. Tous ces Canadiens, après avoir reçu l'habilitation de sécurité requise, se sont attelés à la tâche avec dévouement, énergie, et un sens d'engagement profond. Le Conseil du Trésor a réagi positivement en nous fournissant des ressources limitées mais néanmoins suffisantes. Le Comité, et donc les Canadiens, sont bien servis par ce groupe de professionnels, qui sont leur «agent» et dont les longues heures de travail solitaire ne sont généralement pas reconnues du public, mis à part les efforts que nous avons eu le plaisir de fournir en rédigeant le présent rapport.

* Chambre des communes : *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*, examen de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* : Rapport au Comité permanent de la justice et du solliciteur général, mars 1987.

Annexe A

Directives et instructions ministérielles données au SCRS, 1986-1987

La collaboration entre le SCRS et la GRC touchant l'antiterrorisme

La prestation des évaluations de sécurité

Les avis qui sont transmis au ministre au sujet de certains types d'opérations

L'activité d'enquête

L'utilisation des sources confidentielles

La protection des citoyens canadiens

La protection des citoyens étrangers au Canada

La politique visant les rapports sur les incidents qui sont faits au ministre

Les arrangements à prendre pour obtenir l'aide de la GRC

Annexe B

Résumé des plaintes en matière de sécurité examinées par le Comité de surveillance des activités de renseignement de sécurité, 1986-1987

Habilitations de sécurité

1. Une personne s'est plainte qu'une habilitation au niveau très secret lui avait été refusée parce qu'elle aurait été malhonnête : a) en citant de faux antécédents professionnels sur sa formule de renseignements personnels, b) en détournant la propriété d'un ancien employeur et c) en étant impliquée dans la vente d'objets volés.

À l'audience, le SCRS a cité des rapports de ses sources à l'appui de ces trois allégations. Un enquêteur du SCRS a répondu à des questions détaillées concernant la fiabilité de ces rapports.

Le plaignant a nié toutes les allégations, notant que les déclarations de l'employeur confirmaient l'exactitude des antécédents professionnels et que les autres allégations étaient fondées sur des animosités personnelles. Le plaignant a de plus soutenu que l'allégation concernant la vente d'objets volés résultait d'une erreur d'identité.

Le membre du Comité qui présidait à l'audience a conclu que les antécédents professionnels étaient authentiques, mais il a confirmé les autres allégations.

Il a recommandé de maintenir le refus d'une habilitation au niveau très secret.

2. Un employé s'est vu refuser l'habilitation au niveau très secret dont il avait besoin pour être muté à un service spécial. Le refus était fondé sur des allégations de malhonnêteté, d'indiscrétion, et d'endettement.

On a découvert que l'allégation de malhonnêteté reposait sur un incident mineur et isolé qui ne méritait pas qu'on s'y attarde, et l'indiscrétion s'est révélée sans fondement.

Mais les lourdes dettes étaient réelles, et le SCRS a décidé que les pressions financières qu'elles entraîneraient pourraient tenter le plaignant d'offrir des faveurs aux clients pour de l'argent. Elles pourraient également tenter des clients qui seraient au courant d'offrir des incitations financières.

Toutefois, le SCRS a reconnu que rien n'indiquait que le plaignant ne pourrait pas surmonter ses dettes honnêtement; en fait, il a convenu que les efforts positifs de ce dernier pour résoudre le problème étaient tout à son honneur.

Un agent du ministère employeur a témoigné que, après avoir interrogé le plaignant, il était satisfait de l'explication donnée en regard de la dette.

Jugeant que le plaignant contrôlait très bien sa dette et que toutes les autres allégations étaient sans fondement ou mineures, le membre du Comité qui présidait à l'audience a recommandé l'octroi d'une habilitation au niveau très secret.

Citoyenneté

3. La citoyenneté a été refusée à un immigrant reçu qui était au Canada depuis quatorze ans lorsque le SCRS a affirmé qu'il existait des motifs raisonnables de penser que ce particulier se livrerait à des activités constituant une menace envers la sécurité du Canada.

À l'audience, le SCRS a témoigné que les activités de ce particulier correspondaient à celles d'un agent d'un gouvernement étranger.

Le membre du Comité qui présidait à l'audience a proposé que certaines allégations soient divulguées au requérant et à son avocat de façon à ce qu'une défense raisonnable puisse être préparée. Le membre du Comité qui présidait à l'audience n'a pas cherché à divulguer des faits pouvant nuire à la sécurité nationale mais a insisté sur la divulgation requise par la loi.

Le Service a alors informé le secrétaire d'État qu'il désirait retirer son objection concernant l'octroi de la citoyenneté à ce particulier.

Le membre du Comité qui présidait à l'audience a mis fin à l'enquête puisqu'il n'y avait plus de raison de la poursuivre.

4. Un particulier qui s'est réfugié au Canada après un coup militaire et qui a subséquemment acquis le statut d'immigrant reçu s'est vu refuser la citoyenneté lorsque le SCRS a affirmé qu'il était partisan d'une organisation terroriste dans son pays d'origine.

L'alinéa 2c) de la *Loi sur le SCRS* dispose que les «menaces envers la sécurité» prévoient :

> ...les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes et des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger. (les soulignés sont de nous)

Le requérant et le SCRS étaient chacun représentés par un avocat aux audiences et ils ont tous deux présenté des preuves. Le membre du Comité qui présidait à l'audience a également cité un témoin expert qui a donné des renseignements de base concernant les organisations terroristes dans le pays d'origine du requérant.

Le membre du Comité qui présidait à l'audience a conclu que ce particulier ne menaçait pas la sécurité du Canada, et il a recommandé que la citoyenneté lui soit octroyée.

Au moment de la rédaction du présent rapport, le gouverneur en conseil n'avait pas encore donné suite au rapport du membre du Comité qui présidait à l'audience.

5. Le cas de l'épouse du requérant mentionné dans le cas précédent est également étudié dans cette affaire. Il fait l'objet d'un rapport séparé, mais les faits et les recommandations sont les mêmes. Au moment de la rédaction du présent rapport, le gouverneur en conseil n'avait pas encore donné suite au rapport du membre du Comité qui présidait à l'audience.

6. La citoyenneté a été refusée à un immigrant reçu au Canada depuis 1966 parce que le SCRS croyait qu'il constituait une menace envers la sécurité du Canada. Avant que le Comité ne commence son enquête, le SCRS a retiré sa recommandation voulant que la citoyenneté lui soit refusée.

7. Un particulier qui est entré au Canada à titre de réfugié et a obtenu le statut d'immigrant reçu il y a plus d'une décennie s'est vu refuser la citoyenneté lorsque le SCRS a allégué qu'il était un agent d'influence d'un service de renseignements étranger. Le SCRS a retiré ses objections à l'octroi de la citoyenneté à ce particulier avant que le Comité ne termine son enquête.

Immigration

8. À son entrée au Canada, un particulier a été détenu par les autorités d'immigration, puis relâché le lendemain après avoir comparu devant un arbitre d'immigration.

Le solliciteur général et le ministre de l'Emploi et de l'Immigration ont subséquemment informé le Comité que ce particulier répondait aux critères de déportation énoncés dans la *Loi sur l'immigration de 1976*. Il était spécifiquement allégué que cette personne avait des rapports étroits et actifs avec une organisation terroriste et que sa participation à des actes terroristes était connue.

À l'audience, le SCRS a prouvé ces allégations. La preuve présentée au soutien de celles-ci par le requérant et les témoins manquait de crédibilité.

Le membre du Comité qui présidait à l'audience a conclu qu'il existait des motifs raisonnables de penser que cette personne serait la cause de subversion par la force en regard du gouvernement démocratique d'un autre pays pendant son séjour au Canada, et il a recommandé que des procédures de déportation soient entamées.

Au moment de la rédaction de la présente, le gouverneur en conseil n'avait pas encore donné suite au rapport du membre du Comité qui présidait à l'audience mais le requérant a quitté le pays.

Annexe C

Personnel du Comité au 1er avril 1987

Maurice Archdeacon, secrétaire exécutif	990-6839
Yvette Collins, secrétaire principale	990-8442
Danielle Blache, secrétaire	991-9112
Annie Demirjian, adjointe exécutive	990-6319
Shirley Heafey, agent principal chargé des plaintes	993-4263
Arthur Graham, directeur de la recherche*	990-8051
Maurice M. Klein, agent de recherche	990-8445
John M. Smith, agent de recherche	991-9111
Joan Keane, adjointe de recherche	990-8443
Madeleine DeCarufel, agent administratif et greffier	990-8052
John Caron, agent des dossiers	990-6838
Roger MacDow, commis des dossiers	998-5258
Diane Marion, secrétaire-réceptionniste	990-8441

* Pendant toute la durée de 1986-1987, le directeur de la recherche était Jacques J.M. Shore, qui a démissionné le 31 mars 1987 pour pratiquer le droit à Montréal. Nous désirons le remercier de son apport pendant ses deux années parmi nous.